Data Communication & Client Server Architecture

Network: Connectivity of two or more nodes with the help of wired or wireless media for transmission of data is known as Network.

Networking: It is a process by which a network can be established or maintained.

Internetworking: It is a process by which two or more different network that are based on different subnet of IP address and these networks have been established at same physical location or remote physical location are connected to each other. These locations are known as sites.

Intranet : It is a combination of different networks related to same organization. Ex. – Railway, Defence, Banks, etc.

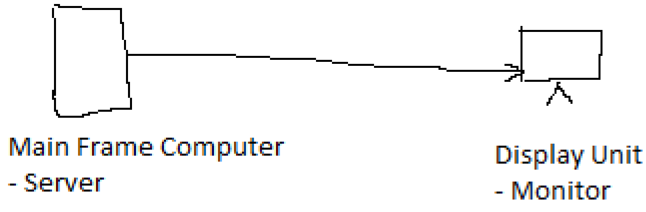
Internet : It is a combination of different networks related to different organization.

Connection Type of nodes :

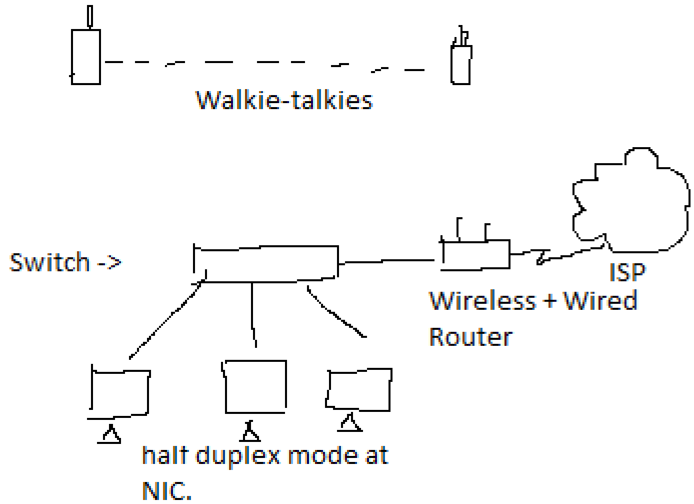
1. **Point-to-point** - Two nodes are connected to a specific link. The whole bandwidth of this link is use by connected two nodes only. Ex. Connection between two laptops, computer connected to a switch, etc.
2. **Point-to-multipoint** – One node is connected to multiple nodes by sharing / dividing the bandwidth of the link. Ex- Connection of multiple branches of a bank to zonal office.

Data Flow :

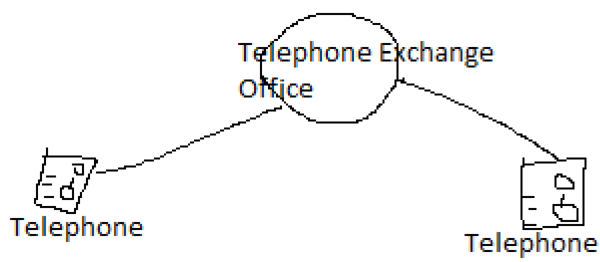
1. **Simplex** - In this transmission sender node always sends data and receiver node only receives data. Ex – Television, Mainframe computer to monitor

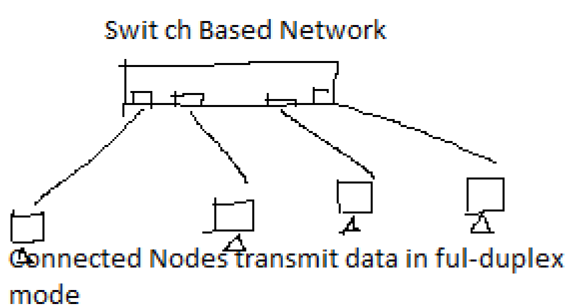


2. **Half Duplex** – In this transmission sender and receiver both can send and receive data but only one task can be done one time. Ex – Walkie-Talkies , Hub



3. **Full Duplex** – In this transmission both sender and receiver can send and receive data at the same time. This is based on channel of transmission medium. Ex- Telephone, Computer, Switch

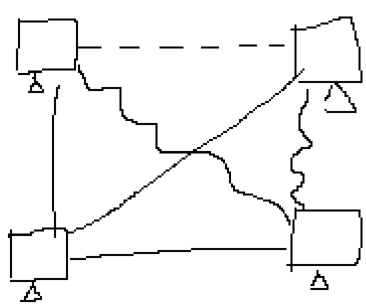




Topology : A network represents connectivity of nodes that is based on physical and logical structure. This structure is known as topology.

Basic Types of topology :

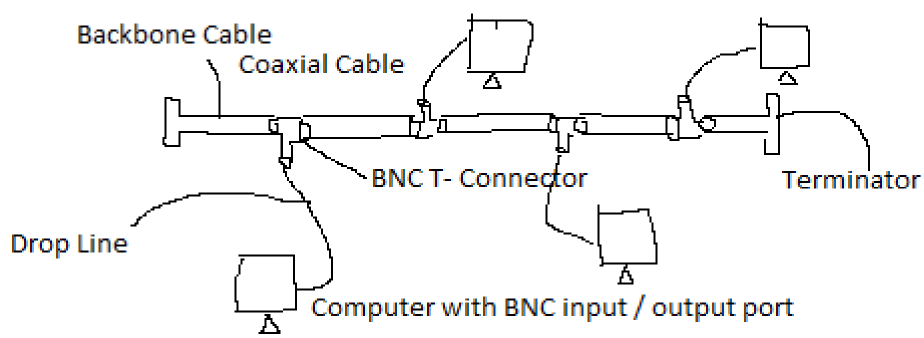
1. **Logical Topology** : It represents the configuration of nodes for different services. Like – OS installation, Services configuration, Logical Addressing (IP address), etc.
2. **Physical Topology** : It represents the arrangement of nodes connected to wired or wireless medium.
   Types of Physical Topology :
   1. **Mesh Topology**
      Important Points :
      a. Each Device is connected to all another device through a dedicated link – point to point connection
      b. Less data traffic load
      c. Failure of one link does not affect another device
      d. It difficult to establish and manage because it requires many links and input / output network ports.
      e. Link Calculation – No. Of nodes (n) = 4
      No. of link to each node = n-1 = 4-1 = 3
      No. Of total link = n(n-1) / 2 = 4(4-1) / 2 = 6
      f. Ex – Telecommunication



Mesh Topology

   2. **Bus Topology**
      Important Points :
      a. All nodes are connected to a single wire (known as back bone cable).
      b. Coaxial Cable is used as a back bone cable.

c. BNC connector is used to at nodes to back bone cable.
d. With the help of BNC , a drop line is created and nodes are connected.
e. At the end of cable Terminator is to used to stop lose of signal.
f. It is easy to establish because it requires less cable and input / output ports.
g. Damage into backbone cable causes failure of connectivity of nodes because break part of cable generates noise for all nodes.
h. Difficult to add a new node.
i. Collision of data is very high.
j. It works on CSMA / CD technique.
k. Ex – Cable TV
l. Each node has information about next node. So, It is known as partial ring topology.
m. It is also known as partial ring topology because each node keeps information about next node.

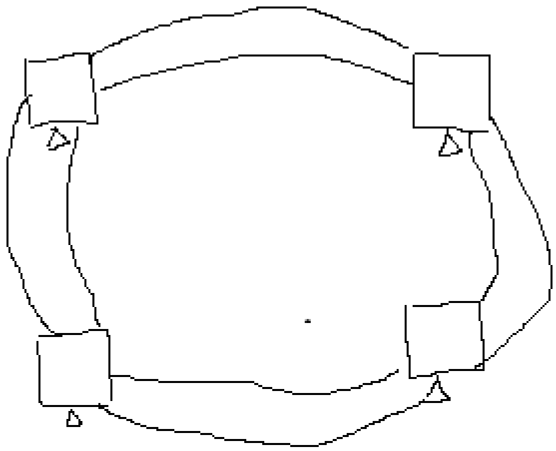


3. Ring Topology

Important Points :

a. Each node is connected to neighbour nodes that forms a ring based structure.
b. Connection can be based on single ring and dual ring.
c. It works on Token Ring Passing technique in which a logical token is transferred from one node to another node. Token is grabbed by the sender node. Sender node add source and destination address with token and released. All data packets are attached behind token. Destination Node accepts this token and extract all attached data packets.
d. It reduces data confliction.

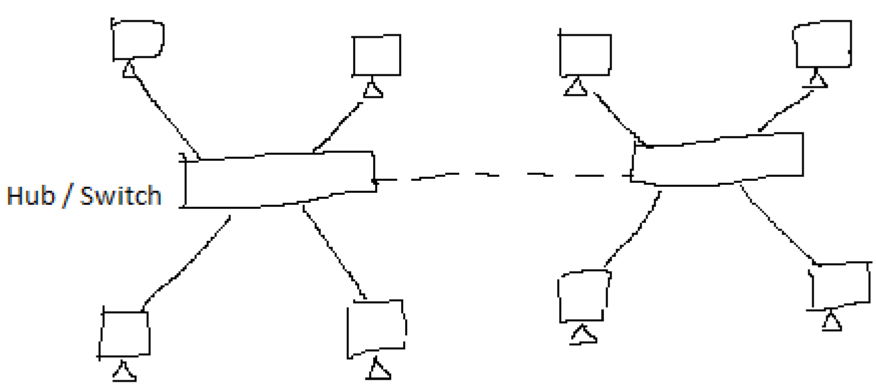
e. Max. Two links are used.
f. It is very slow.



4. Star Topology

Important Points :

a. In this topology each node to connected to a central device that is known as MAU (Multiple Access Unit). MAU can be Hub or Switch.
b. Each node is connected to MAU with separate link.
c. Performance of this topology depends upon MAU and link quality.
d. If problem occur with any node, it does not affect another nodes means reliability is very high.
e. It is most commonly used topology in LAN.



Star Topology

5. Wireless Topology

Important Points :

a. In this topology, unguided media is used.
b. It works on frequency. Commonly in LAN – 2.4 GHz or 5 GHz
c. All nodes are connected to a central device that is known as AP (Access Point)
d. AP name is known as SSID (Security Set Identifier)
e. This topology can be extended easily.
f. Wireless Security Protocols :

   Wired Equivalent Privacy (WEP)
   Wi-Fi Protected Access (WPA)
   Wi-Fi Protected Access 2 (WPA 2)
   Wi-Fi Protected Access 3 (WPA 3)

   WEP (Wired Equivalent Privacy) – It was developed for wireless networks and approved as a Wi-Fi security standard in September 1999. WEP was supposed to offer the same security level as wired networks, however there are a lot of well-known security issues in WEP, which is also easy to break and hard to configure. Despite all the work that has been done to improve the WEP system it still is a highly vulnerable solution. Systems that rely on this protocol should be either upgraded or replaced in case security upgrade is not possible. WEP was officially abandoned by the Wi-Fi Alliance in 2004.

WPA (Wi-Fi Protected Access)- For the time the 802.11i wireless security standard was in development, WPA was used as a temporary security enhancement for WEP. One year before WEP was officially abandoned, WPA was formally adopted. Most modern WPA applications use a pre-shared key (PSK), most often referred to as WPA Personal, and the Temporal Key Integrity Protocol or TKIP (/tiːˈkɪp/) for encryption. WPA Enterprise uses an authentication server for keys and certificates generation.

WPA was a significant enhancement over WEP, but as the core components were made so they could be rolled out through firmware upgrades on WEP-enabled devices, they still relied onto exploited elements.

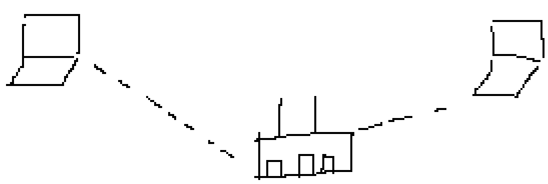
WPA, just like WEP, after being put through proof-of-concept and applied public demonstrations turned out to be pretty vulnerable to intrusion. The attacks that posed the most threat to the protocol were however not the direct ones, but those that were made on Wi-Fi Protected Setup (WPS) - auxiliary system developed to simplify the linking of devices to modern access points.

WPA2 (WPA version 2)

The 802.11i wireless security standard based protocol was introduced in 2004. The most important improvement of WPA2 over WPA was the usage of the Advanced Encryption Standard (AES). AES is approved by the U.S. government for encrypting the information classified as top secret, so it must be good enough to protect home networks.

ADVANCED ENCRYPTION STANDARD IS APPROVED BY THE U.S. GOVERNMENT

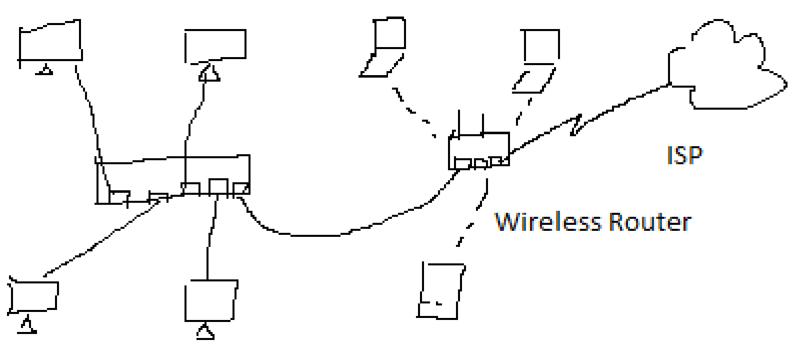
At this time the main vulnerability to a WPA2 system is when the attacker already has access to a secured WiFi network and can gain access to certain keys to perform an attack on other devices on the network. This being said, the security suggestions for the known WPA2 vulnerabilities are mostly significant to the networks of enterprise levels, and not really relevant for small home networks.
Unfortunately, the possibility of attacks via the Wi-Fi Protected Setup (WPS), is still high in the current WPA2-capable access points, which is the issue with WPA too. And even though breaking into a WPA/WPA2 secured network through this hole will take anywhere around 2 to 14 hours it is still a real security issue and WPS should be disabled and it would be good if the access point firmware could be reset to a distribution not supporting WPS to entirely exclude this attack vector.



Wireless Router

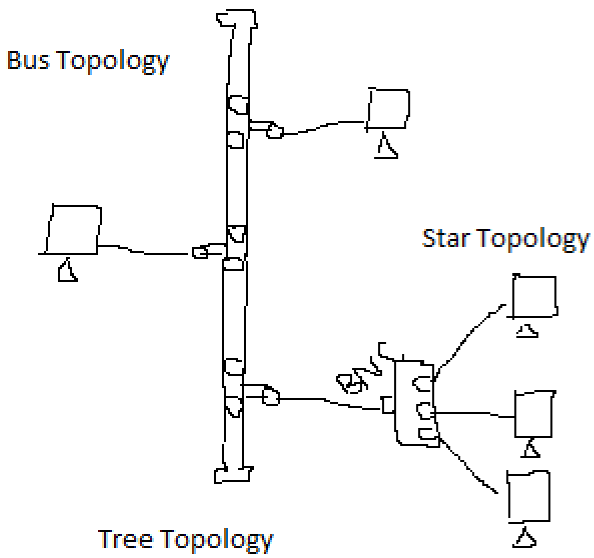
6. Hybrid Topology

It is just the combination of two or more topologies.



Hybrid Topology

7. **Tree Topology**
   It is combination of Bus and Star topology.

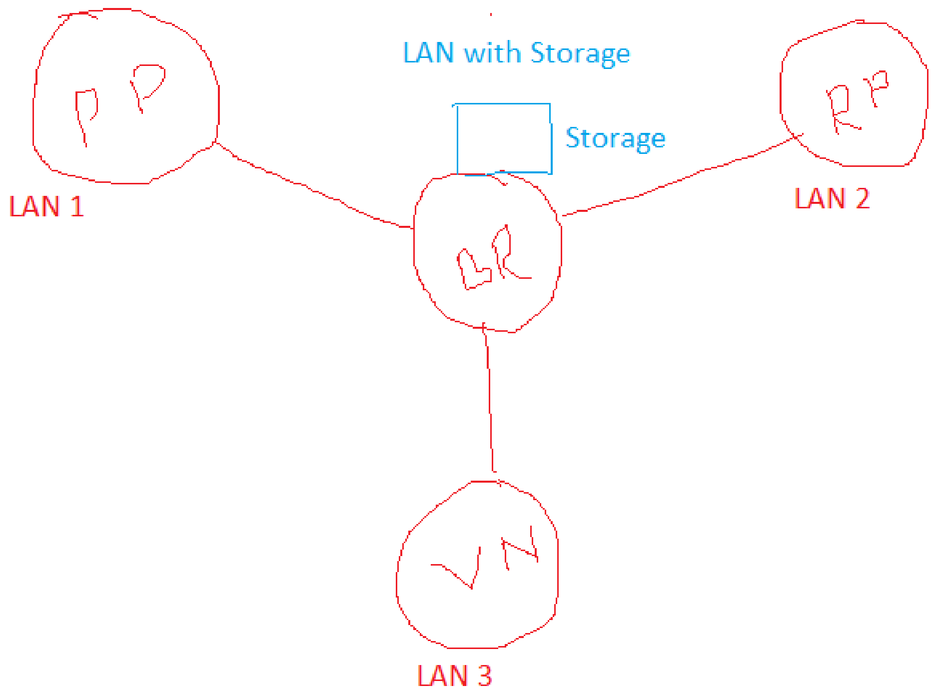


Categories of Network :

1. **LAN**
   A network that has been established in a small area like small office, corporate office, building or campus is known as LAN (Local Area Network). It is mostly based on twisted pair cable or wireless.

2. **MAN**
   A network that has been established in a large city (Metropolitan City) like Internet connection, government project etc. Is known as MAN (Metropolitan Area Network). It can be based on Optical Fiber Cable or Frequency.

3. **WAN**
   A network that has been established in very large area like country or world. It is mostly combination of multiple organizations network. Ex. – Internet
4. **SAN (Storage Area Network)**
   A network that is used to store huge amount of data is known as SAN.

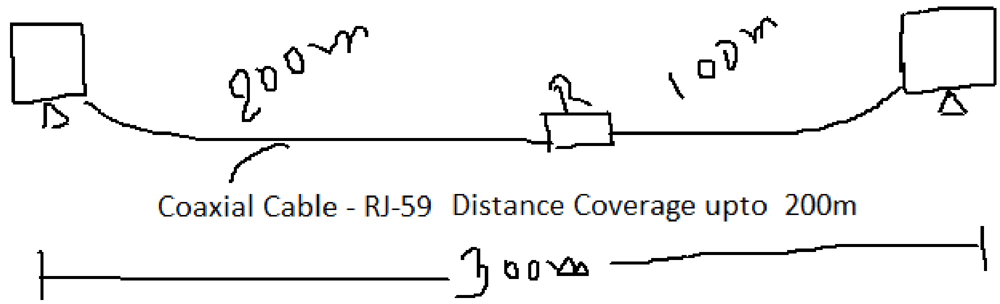


5. CAN (Campus Area Network)
6. PAN (Personal Area Network)

Basic Concept of Devices :

The above transmission of data, topology and network models are developed with the help of few devices :

1. **Repeater –** It is used to regenerate weak data signal with its original strength. Repeater is used with media for long transmission of data signal.
   Ex- Coaxial Cable (RJ-59 / Thin Coaxial Cable) – Distance Coverage →upto 200m



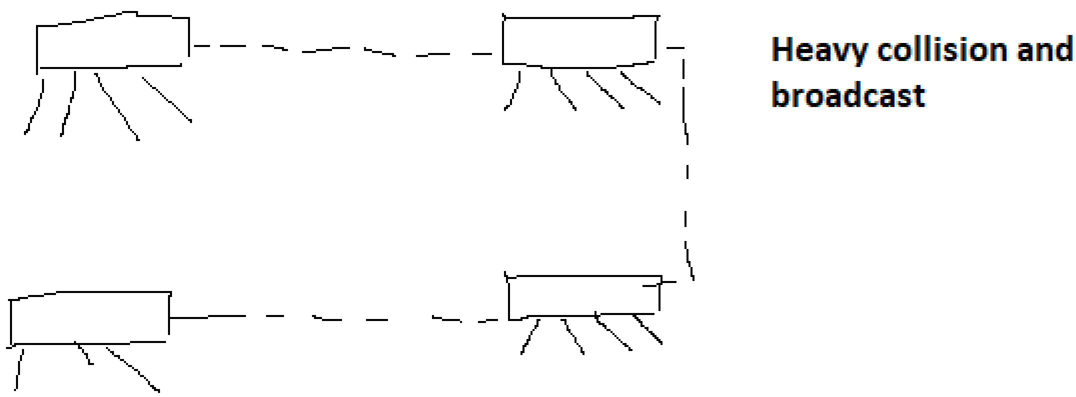
2. NIC (Network Interface Card) / LAN Card / Network Card /Ethernet Card

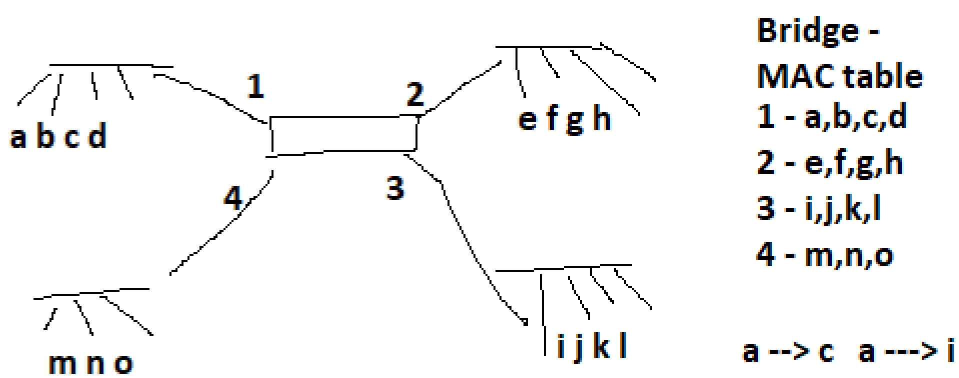
a. Works at layer 2 – Data Link layer
b. Used to connect a node with another node or network
c. Types – wired , wireless
d. At wired NIC RJ-45 port is available with 8 pins
e. Wireless NIC works at frequency (Radio Frequency)
f. NIC has a ROM in which MAC address is present. So, MAC address is known as Physical Address.
g. By default NIC works in auto mode while it can be set for Half Duplex or Full Duplex mode.
h. Mostly NIC is with fixed with mother board. In case of extra NIC, it is attached with PCI slots.

3. Hub

a. Hub is used in star topology
b. It just connect multiple nodes as a connector
c. Works at physical layer
d. RJ – 45 ports - 4, 8,16,24
e. Heavy collision and broadcasting
f. It works in half duplex mode
g. Maximum speed – 10 Mbps
h. Types of HUB – Active , Passive
Passive – Data signal is weak
Active – Works as multiport repeater. Signal is regenerated at every port.

4. **Bridge**
    a. Used in star topology based network.
    b. OS based device
    c. Creates MAC address table
    d. It works at data link layer
    e. Available with 2 or 4 RJ-45 ports
    f. Reduces collision and broadcast
    g. It is used to break a network into segments or to join multiple segments of network.





5. **Switch**
    a. This device is used in star topology based network.
    b. It is almost similar to Hub in structure.
    c. It has RJ-45 ports.
    d. It is available with 4, 8, 16, 24, 48, 96, 128 ports.
    e. Switches are available with 100Mbps, 1000Mbps or 10Gbps speed
    f. It works in full duplex mode

g. Switch works at layer 2 and layer 3 both. So, Switches are also known as Layer 2 or 3 switch.

h. It has multiple broadcast domain and collision domain. But switch initially works in single broadcast domain till the learning of MAC address.

i. It creates MAC Table / CAM table /Filter Table

Types of Switch :

1. **Unmanageable Switch –** It is just plug and play device. It cannot be configured.
2. **Manageable Switch –** It can be configured for port management, IP address configuration , security, etc.

6. Router

a. Router is used for communication between two or more different network that are based on different subnet of IP address.
b. It is a Layer 3 device.
c. It is an OS based device.
d. It creates routing table in which it keeps best route information for different destination network.
e. It can filter data packets.
f. It has different types of ports like Fast Ethernet, Gigabyte Ethernet, serial port, ISDN port, Console port, etc.

Types of Router :

1. **De-modular Router –** Its all ports are fixed with router. Ex. – Model 2520
2. **Modular Router –** Its few ports are fixed with router and some free slots are available to attach different types of cards. Ex. – Model 1841, 1941, 7200, 900, 901

7. Firewall

a. This device is used for security in the network.
b. It can filter data packets.
c. It allows or restricts different sites.
d. It can also route data packets.
e. It is an OS based device.

f. It can be implemented at the boundary of network or in the middle of network.
g. It has different types of ports like router.
h. Ex – ASA 5500

8. **Access Point**
    - **a.** This device is used to create a wireless network.
    - **b.** It generates signal through which wireless devices are connected to it.
    - **c.** It has internet port, fast Ethernet or Giga Byte Ethernet ports.
    - **d.** It supports MAC filtering, Port forwarding, speed control, data use limitation, etc.

Media

A path through which data can be transmitted.

Types – Guided Media – Wired Communication

Unguided Media – Wireless Communication

Frequency based data transmission.

Network Cables

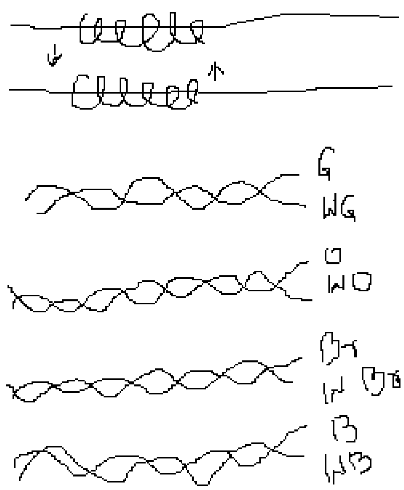
1. Twisted Pair Cable (TPC)
    - a. 4 pair Cable – 8 cables
    - b. Based on Ethernet Technique (IEEE – 802.3)
    - c. Uses – Computer Network, CCTV, Telephone, Wi-Fi devices, V-SAT
    - d. Speed – up to 1 Gbps
    - e. Distance Coverage – up to 100m
    - f. Connector – RJ-45 (RJ- Registered Jack) – 8 pins
      RJ-11 - 4 pins (Modem, Tel. Set)
    - g. Categories – cat1,2,3,4,5,5e,6,6a,7
    - h. Types –
        1. STP – Very less effect of EMI
        2. UTP - High effect of EMI
    - i. Cable Color code given by TIA/EIA
        - a. Pair 1 – Orange, White Orange
        - b. Pair 2 – Blue, White Blue
        - c. Pair 3 – Green, White Green
        - d. Pair 4 – Brown, White Brown

Total pairs 4 = 8 wires

j. Twisted Pair Cable pairs are managed to create different cable as per used by arranging is cable color –
   1. Straight Over Cable – Used to connect dissimilar devices like – Computer to hub or switch, Router to switch, firewall to switch/router
   2. Cross Over Cable – Used to connect similar devices like – Router to Router, Hub to Hub, Switch to Switch, PC to PC
   3. Roll Over Cable – Used to connect Router, Firewall or Switch with PC for configuration

      Now, the above cables are based on sequence of color of cable in the connector.

Why twisting is done with TPC?



TIA/EIA has given few standard for sequencing of cable –

TIA/EIA-T568A			TIA/EIA-T568B	
1	WG		1	WO
2	G		2	O
3	WO		3	WG
4	B		4	B
5	WB		5	WB
6	O		6	G
7	Br		7	Br
8	WBr		8	WBr

1. Straight Over Cable –

Use 568A or 568B rule at both end of cable.

2. Cross Over Cable –
   Use 568A rule at one end and 568B rule at another end.
   OR,
   Use 568B rule at one end and 568A rule at another end.
3. Roll Over Cable –
   We can use 568A or 568B rule at one end but at another end just opposite the position of cable.

WO	Br	Roll Over Cable sequence.
O	WBr	
WG	G	
B	WB	
WB	B	
G	WG	
WBr	O	
Br	WO	

Patch Code – Industry manufactured TPC with connector.
Practical - [RJ45 plug on UTP cable - Installing - YouTube]

Coaxial Cable:-

1. Single copper wire.
2. Proper shielded
3. Connector – BNC
4. Distance Coverage – up to 500m
5. Speed – 10Mbps
6. Uses – Cable TV, Bus Topology based network, CCTV
7. Types:
   a. RG-58 / Thick Coaxial Cable / 10Base5
   b. RG-59 / Thin Coaxial Cable / 10Base2
8. To connect PC with coaxial cable, PC must have BNC port.

Optical Fiber Cable / Fiber Optic Cable (OFC)/Fiber Cable

1. Light – Laser / LED
2. Small Diameter
3. Works on total internal reflection
4. Glass / Fiber
5. Long distance
6. Speed high
7. Flexible -

8. Bandwidth high
9. Costly
10. Light moves in straight line
11. Tough use
12. Very less effect of EMI
13. Patch Code

What is protocol?

It is a set of rules and instructions which is responsible to execute a specific process.

Initially protocols are platform dependent.

To make protocols platform independent, TCP/IP Model was developed by Department of Defense of America. So, It is also known as DOD model.

It has 4 / 5 layers :

4 Application – OSI Ref. Model –App, Pre, Session
Protocols – DNS, DHCP, HTTP, HTTPs, POP3, IMAP
3 Transport - Protocols –TCP, UDP

2 Internet - OSI Ref. Model – Network Layer

Protocols – IP, ICMP,

1 Network Interface – OSI Ref. Model – Data Link & Physical Layer

MPLS, Ethernet, Frame Relay, ATM,

OR,

5 Application

4 Session

3 Transport

2 Network

1 Physical

To explain TCP/IP model in more detail, OSI Model was developed.

So, it is also known as OSI Reference Model.

Protocols –

1. HTTPs (Hyper Text Transfer Protocol with SSL(Secure Socket Layer) - 443
   Used for web page accessing with security
2. HTTP (Hyper Text Transfer Protocol) - 80
   Used for web page accessing without security
3. FTP (File Transfer Protocol) – 20,21

4. DHCP (Dynamic Host Configuration Protocol) – 67,68
   Used to provide IP address automatically and dynamically to client machines as per configuration.
   Practical:
5. DNS (Domain Name Service / System) - 53
   Used to convert Domain name to IP address and vice versa
   Practical:
6. SMTP (Simple Mail Transfer Protocol) - 25
   Used for mail service. In mail service, it is used to transfer mail.
7. POP3 (Post Office Protocol version 3) - 110
   Used to receive mail. In case of Outlook, it cuts mail from mail server and download it on local machine.
8. IMAP4 (Internet Message Access Protocol) - 143
   Used to receive mail. In case of Outlook, it copies mail from mail server and download it on local machine.
9. Telnet (Tele Comminication) - 23
   It is used to access a machine remotely through command line.
   Practical:
10. RDP (Remote Desktop Protocol)
    It is used to access a machine remotely with GUI.
    Practical:
11. SSH (Secure Shell) -22
    It is used to access a machine remotely with command line. It provides high security with MD5 (Message Digest version 5) encryption.
12. TCP (Transmission Control Protocol)
    Used for reliable data transmission with acknowledgement.
13. UDP (User Datagram Protocol)
    Used for unreliable data transmission without acknowledgement.
14. IP (Internet Protocol)
    It is used to provide unique identity to network nodes.

With this identity, two or more nodes of a network or different network can communicated to each other.
Version – IPv4, IPv6

15. ICMP (Internet Control Message Protocol) - 1
It is used to send and receive data packetes to check connectivity with destination node.
Practical:

16. ARP (Address Resolution Protocol)
It resolves MAC address with IP address.
Practical:

17. WAN Technics –Leased Line, ISDN
Frame Relay, ATM, MPLS, VoIP

Characteristics of OSI Model

Here are some important characteristics of the OSI model:

- A layer should only be created where the definite levels of abstraction are needed.
- The function of each layer should be selected as per the internationally standardized protocols.
- The number of layers should be large so that separate functions should not be put in the same layer. At the same time, it should be small enough so that architecture doesn't become very complicated.
- In the OSI model, each layer relies on the next lower layer to perform primitive functions. Every level should able to provide services to the next higher layer
- Changes made in one layer should not need changes in other lavers.

Why of OSI Model?

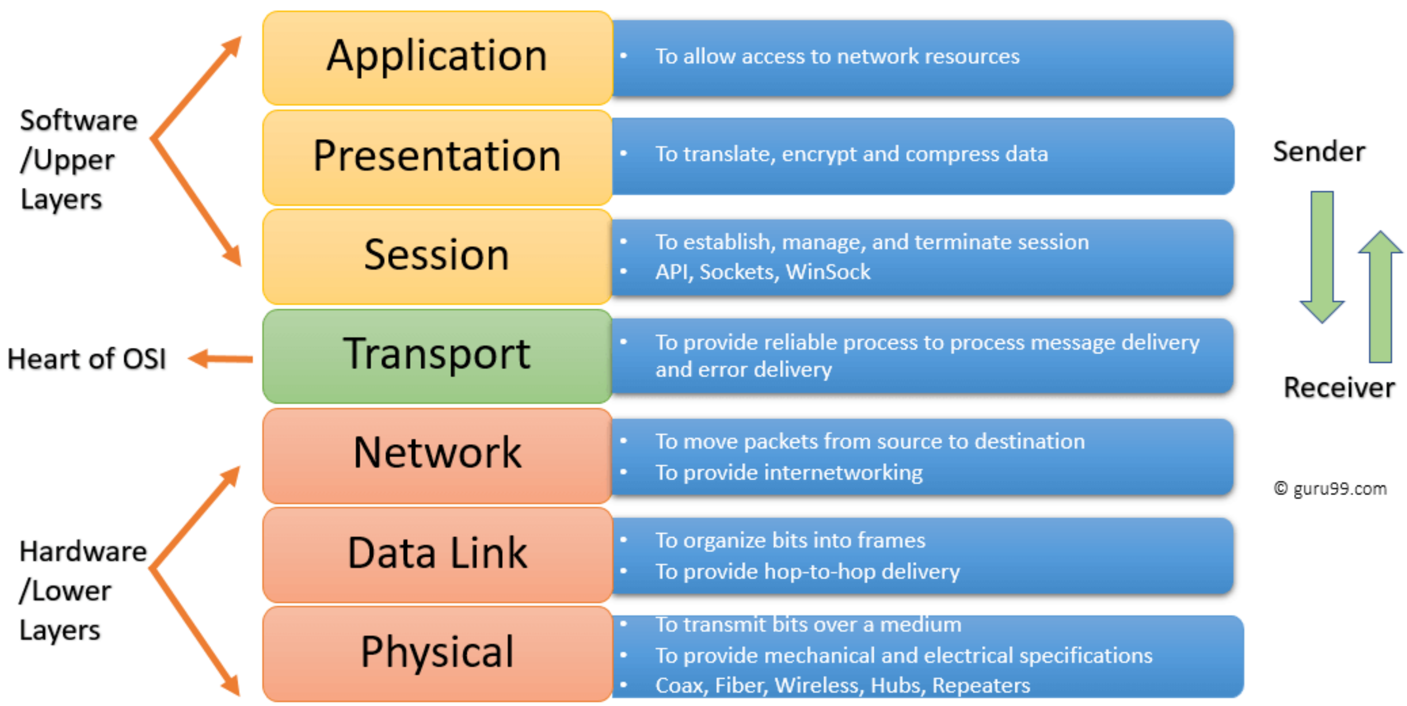
- Helps you to understand communication over a network
- Troubleshooting is easier by separating functions into different network layers.
- Helps you to understand new technologies as they are developed.
- Allows you to compare primary functional relationships on various network layers.

History of OSI Model

Here are essential landmarks from the history of OSI model:

- In the late 1970s, the ISO conducted a program to develop general standards and methods of networking.
- In 1973, an Experimental Packet Switched System in the UK identified the requirement for defining the higher-level protocols.
- In the year 1983, OSI model was initially intended to be a detailed specification of actual interfaces.
- In 1984, the OSI architecture was formally adopted by ISO as an international standard

7 Layers of the OSI Model



Physical Layer

The physical layer helps you to define the electrical and physical specifications of the data connection. This level establishes the relationship between a device and a physical transmission medium. The physical layer is not concerned with protocols or other such higher-layer items.

Examples of hardware in the physical layer are network adapters, ethernet, repeaters, networking hubs, etc.

Few important Points:

a. Physical characteristics of interfaces and medium
b. Representation of bits
c. Data rate
d. Synchronization of bits
e. Line configuration
f. Physical topology
g. Transmission mode

Data & Signal

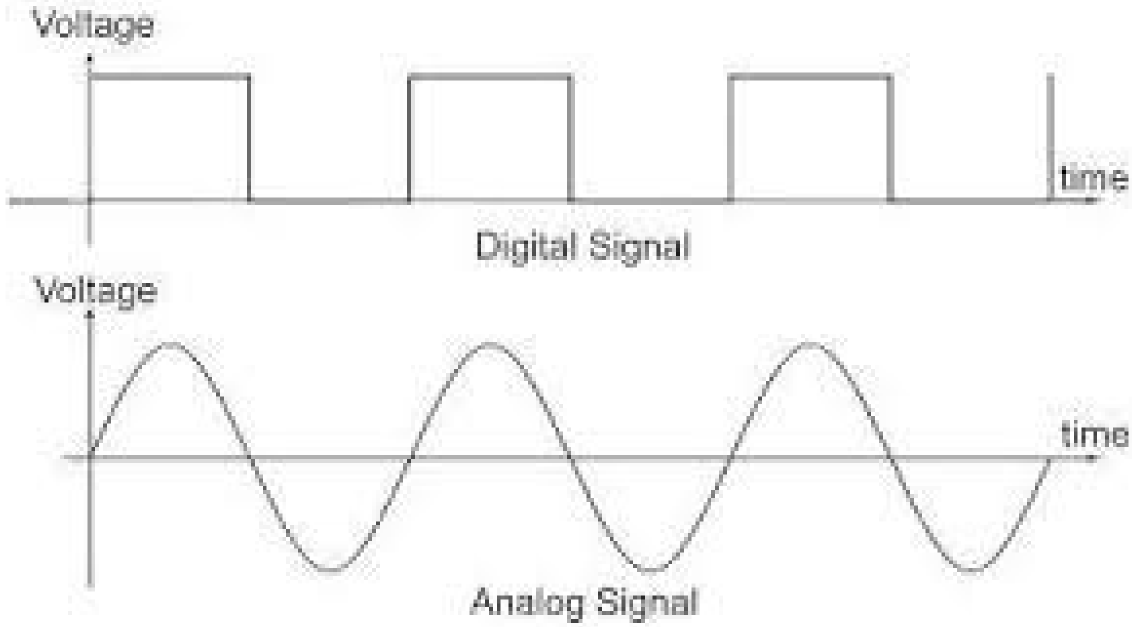
Data can be analog or digital that communicate at a medium or stored at a device.
Analog Data - Continuous flow of data like voice.
Digital Data - Break in the flow of data like data stored in the computer in the form of 0's and 1's.
Signal : It is carrier of data.

Analog Signal :

1. It has infinite number of values.
2. It has continuous flow of electrical signal.
3. It is represented into sine waves.

Digital Signal :

1. It has only 2 values that is 0's and 1's.
2. It has non-continuous electrical signal.
3. It is represented into square waves.



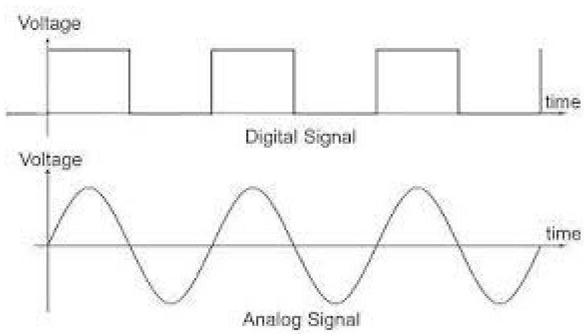
Periodic and non-periodic / Aperiodic Signal

Both analog and digital signal can be periodic and non-periodic signal.

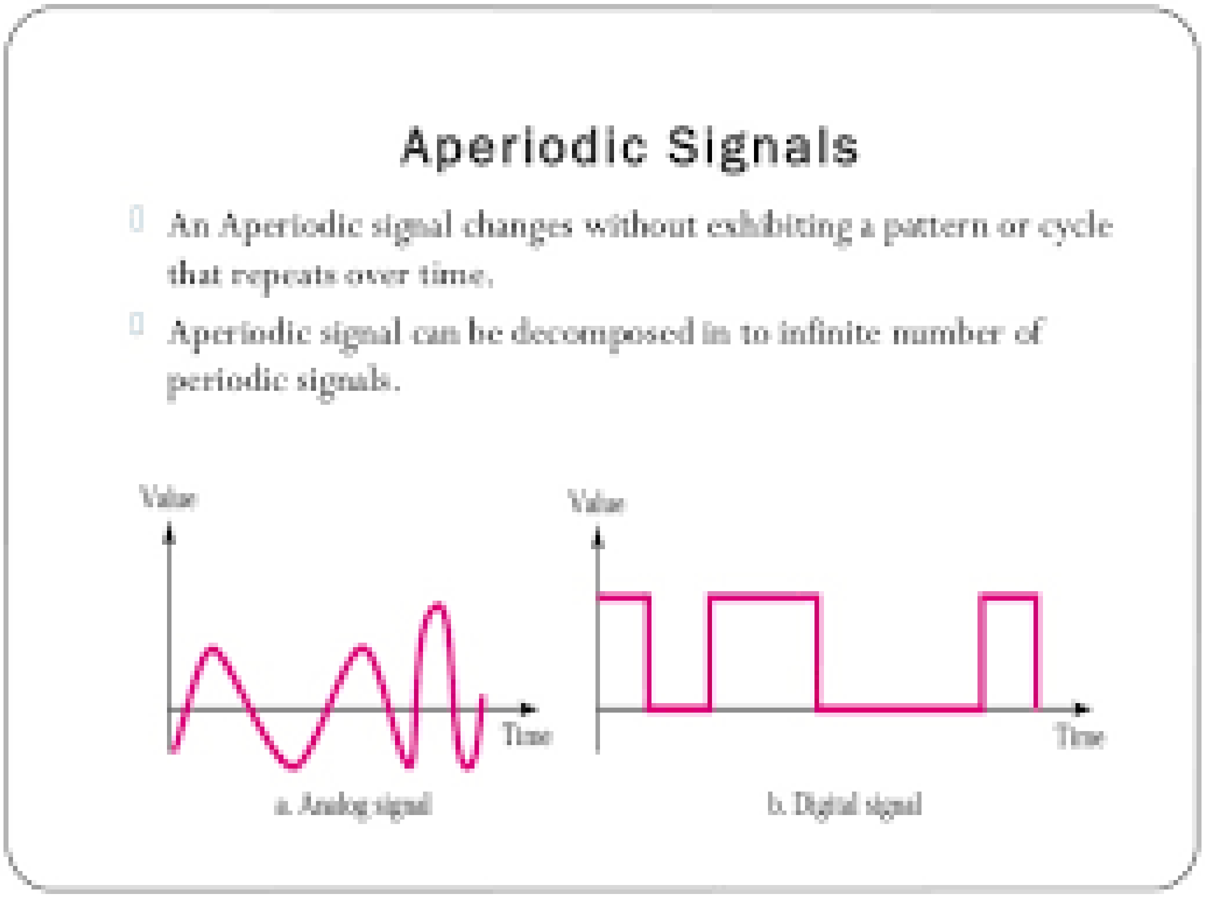
A periodic signal completes the same cycle at fixed interval of time.

A non-periodic signal does not complete its cycle at fixed interval of time.

Example of periodic signal :



Example of non-periodic signal :



Few Properties of Sine Wave (Analog Signal):

1. Amplitude : The highest peak of signal is known as its amplitude. In case of electrical signal it is measured in Volt (V).
2. Period : One cycle of signal is known as 1 period. It is measured in Second.
3. Frequency : Number of period in 1 S. It is measured in Hertz (Hz).

Notes : Frequency and period are the inverse of each other.

f=1/t   or t=1/f

Unit	Equivalent	Unit	Equivalent
Seconds(S)	1s	Hertz (Hz)	1Hz
Millisecnds(ms)	10-3s	Kilohertz(KHz)	10^3 Hz
Microseconds(ms)	10-6s	Megahertz(MHz)	10^6 Hz
Nanoseconds(ns)	10-9s	Gigahertz(GHz)	10^9 Hz
Picoseconds	10-12s	Terahertz(TH	10^12 Hz

(ps)		z)	

4. Wavelength : Distance between two crests or troughs is known as wavelength. It is measured in lamda.
5. Phase : Two or more waves with same frequency, amplitude and wavelength but its point of generation degree is different.
6. Single Sine Wave - It is a single signal means only one sine wave is generated from one device to another. It is used to carry electric supply, alarm etc.
7. Composite Signal - It is a combination of multiple sine waves. It type of signal is used to carry data.

Few properties of Digital Signal

1. Uses electric low and high voltage to represent data.
2. Data is represented in 0's and 1's.
3. Speed of digital signal is measured in bits per seconds that is known as bit rate.
4. Low Pass Channel - A channel that starts with 0.

Bandwidth :

The range of frequencies contained in a composite signal is its bandwidth.

The bandwidth is normally a difference between two numbers. For example, if a composite signal contains frequencies between 1000 and 5000, its bandwidth is 5000 - 1000, or 4000.

Throughput:-

The throughput is a measure of how fast we can actually send data through a network.

Although, at first glance, bandwidth in bits per second and throughput seem the same,
they are different. A link may have a bandwidth of *B* bps, but we can only send *T* bps
through this link with *T* always less than *B*. In other words, the bandwidth is a potential
measurement of a link; the throughput is an actual measurement of how fast we can
send data. For example, we may have a link with a bandwidth of 10 Mbps, but the

devices connected to the end of the link may handle only 5 Mbps. This means that we
cannot send more than 5 Mbps through this link.

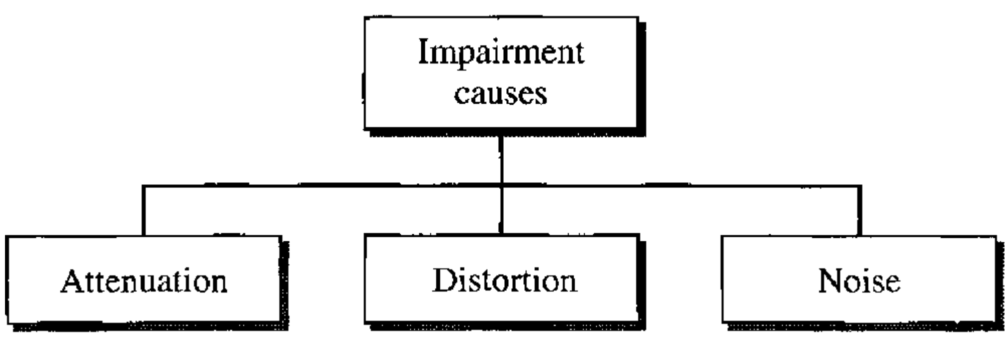
Baseband transmission –

1. Digital signaling.
2. Time division multiplexing is used
3. Baseband is bi-directional transmission by using TDM.
4. Short distance signal travelling.
5. Entire bandwidth is for single signal transmission.
6. Example: Ethernet – 10BaseT

Broadband transmission –

1. Analog signaling.
2. Frequency division multiplexing possible
3. Transmission of data is unidirectional by using FDM. FDM is used to create multiple channels.
4. Long distance signal travelling.
5. Bandwidth is divided into multiple channels.
6. Example : Used to transmit cable TV, Telephone, Radio Station, Fiber Optic Cable

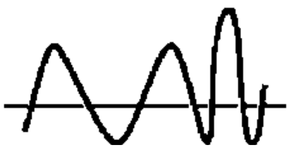
Transmission Impairment : Simply we can say, it is disturbance with data signal during the transmission through medium. Due to impairment, data loss occurs.



a. Attenuation -
Attenuation means a loss of energy. When a signal, simple or composite, travels
through a medium, it loses some of its energy in overcoming the resistance of the

medium. That is why a wire carrying electric signals gets warm. Some of the electrical energy in the signal is converted to heat. To compensate for this loss, amplifiers are used to amplify the signal.

Original Signal



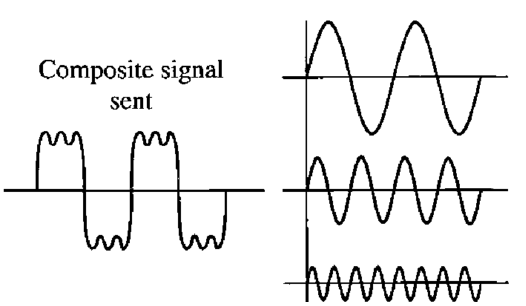
Attenuated Signal

Amplified Signal

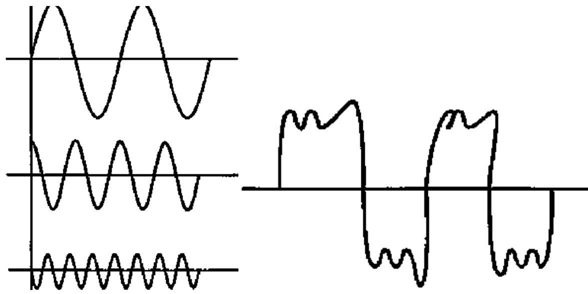
Note : Signal strength is measured in decibel (dB).

Distortion

Distortion means that the signal changes its form or shape. Distortion can occur in a
composite signal made of different frequencies and phase. Each signal component has its own
propagation speed through a medium. So, distortion may cause of delay in transmission and loss of data.



Three signals with different phases.

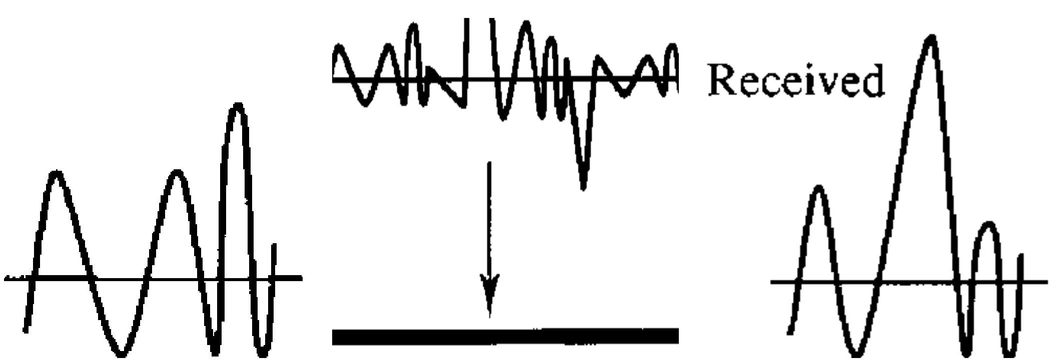


This is distorted received signal.

Composite Signal Received

Noise

Noise is another cause of impairment. Several types of noise, such as thermal noise,
induced noise, crosstalk, and impulse noise, may corrupt the signal. Thermal noise is
the random motion of electrons in a wire which creates an extra signal not originally
sent by the transmitter. Induced noise comes from sources such as motors and appliances.
These devices act as a sending antenna, and the transmission medium acts as the
receiving antenna. Crosstalk is the effect of one wire on the other. One wire acts as a
sending antenna and the other as the receiving antenna. Impulse noise is a spike (a signal
with high energy in a very short time) that comes from power lines, lightning, and so on.



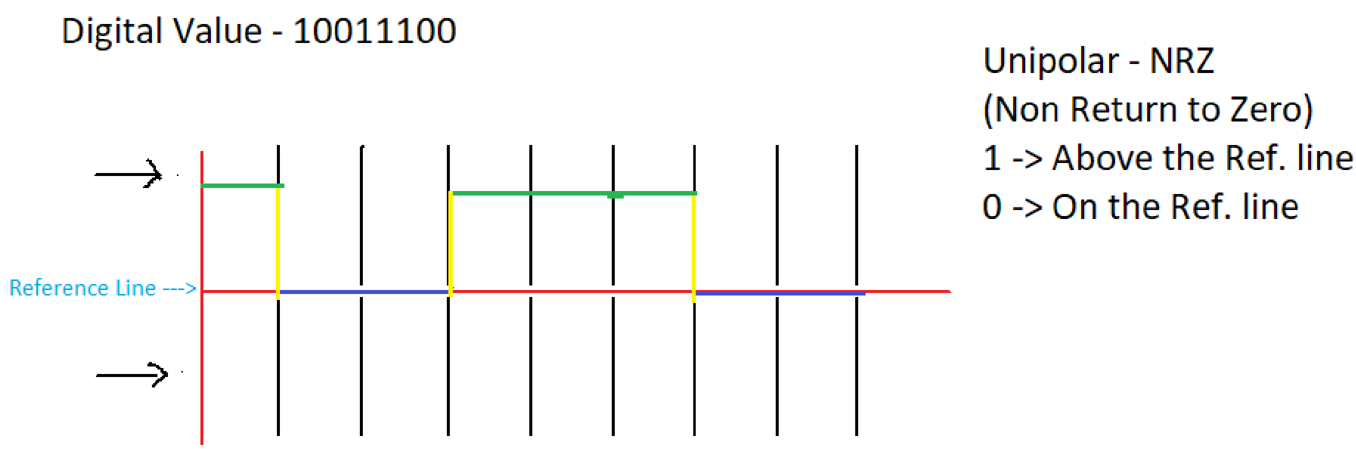
Sent Signal Noise generated Distorted Signal

Digital Data over Digital SIgnal :

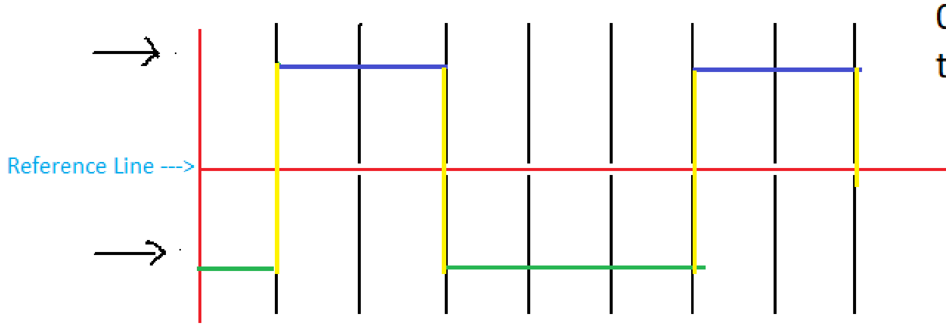
Line Coding :
Putting digital data over digital signal is known as Line Coding.

There are 5 major categories of Line Coding :
1. Unipolar - NRZ
2. Polar - NRZ-L, NRZ-I, RZ, Manchester, Differential Manchester
3. Bipolar – RZ, AMI, pseudoternary
4. Multilevel - 2B/IQ
5. Multi transition - MLT-3

Example of few line coding:-

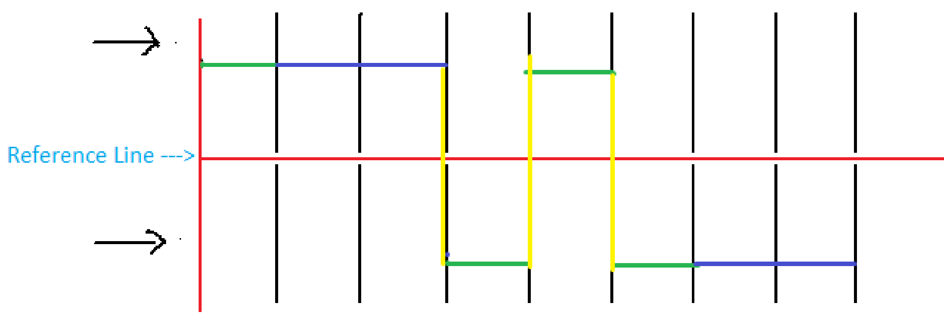


Digital Value - 10011100



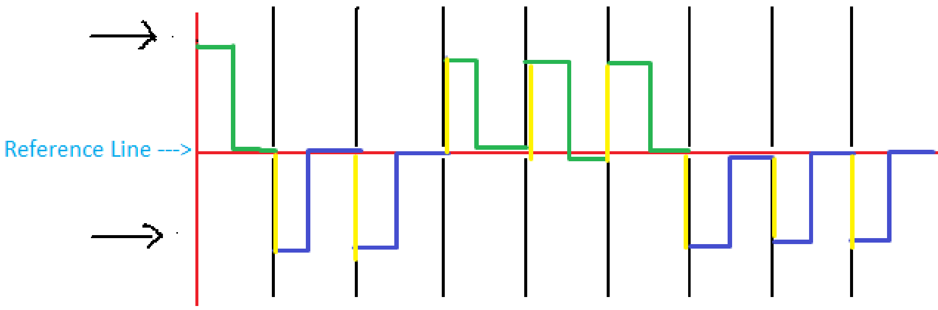
NRZ-L -> 1 is represented below the Ref. line.
0 is represented above the Ref. line.

Digital Value - 10011100

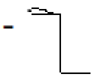


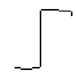
Polar - NRZ-I
O or 1 both can be represented above the Ref. line.
O - No Transition
1 - Transition

Digital Value - 10011100

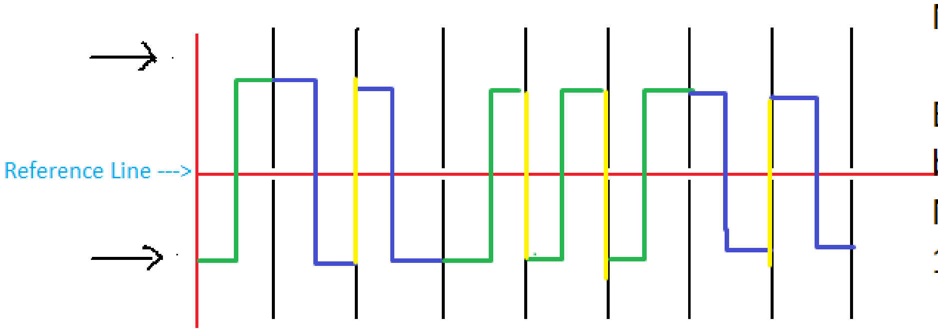


Polar - RZ(Return To Zero)
Transition will occour between the bit to represent every bits.

1 - Above the Ref. Line
Symbol - 

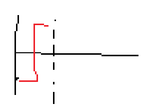
0 - Below the Ref. Line
Symbol - 

Digital Value - 10011100

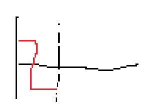


Polar-Manchester
(Based on IEEE-802.3)
Notes :- Above RL, +ve
Below RL , -ve
Every bit wil transite between bits.
Now,

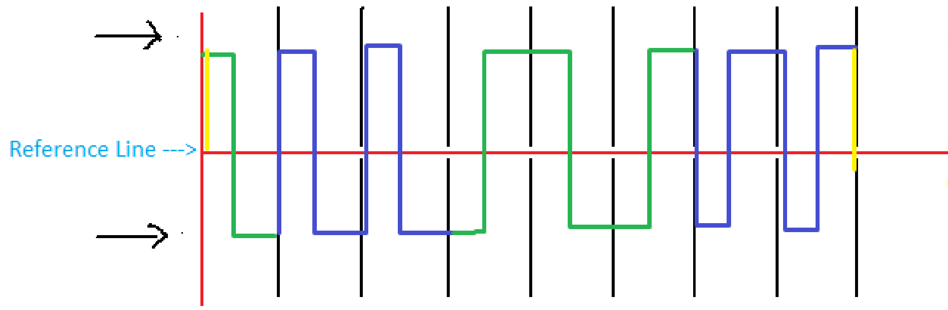
1 - Transition -ve to +ve



0 - Transition +ve to -ve



Digital Value - 10011100

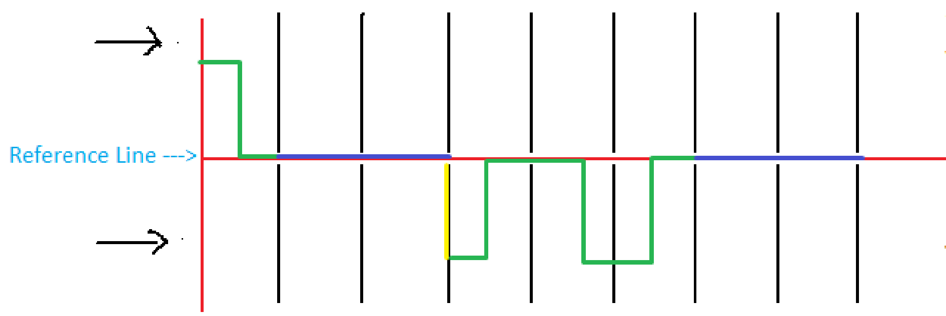


Polar - Differential
Manchester (D-Man)
Transition occour at every bit i.e. 0 ro 1
Both are represented above and below the RL.
0 - symbol

1 - Symbol

These symbols are used as per the situation.

Digital Value - 10011100



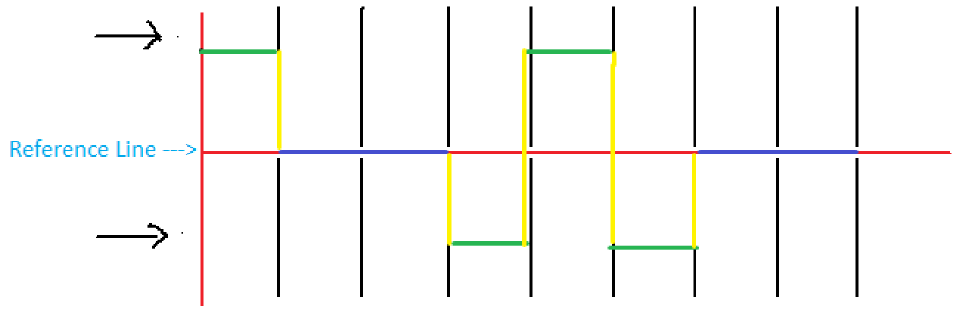
Bipolar - RZ(Return To Zero)
1 - It can be represented above or below the Ref. Line with symbol

If first 1 is represented with

then the next 1 is with

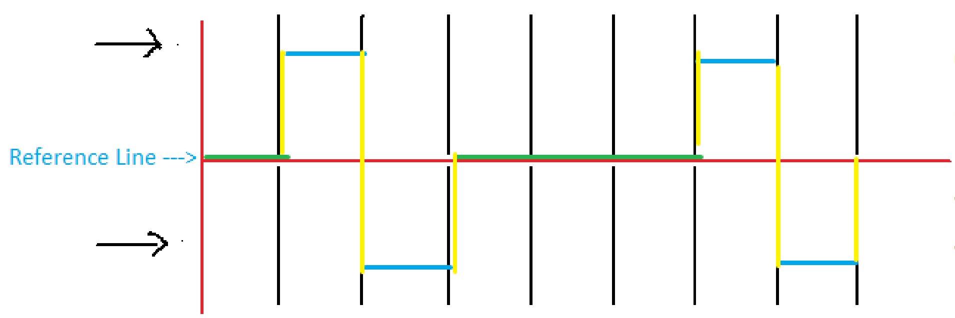
0 - Always represented on the Ref. Line.

Digital Value - 10011100



Bipolar- AMI or NRZ
AMI - Alternate Mark Inversion
0- Always represented at Ref. Line
1- represented above or below the RL. But it should be alternate means if first 1 is above the RL then second 1 will be below the RL then the next 1 will be above the RL and so on.

Digital Value - 10011100

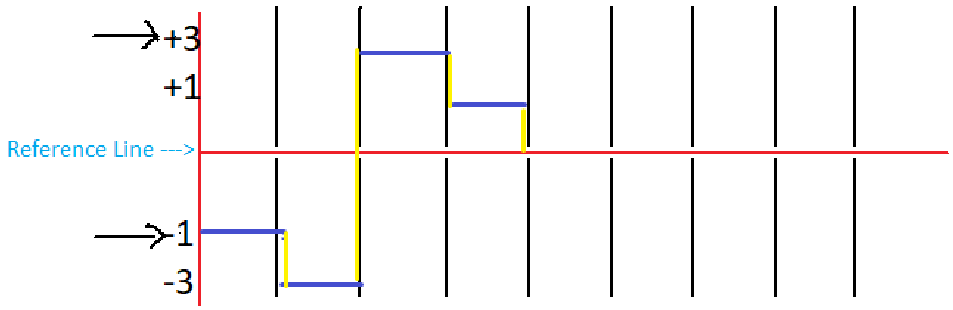


Bipolar-Pseudoternary
1 - It is always represented on the RL.
0 - It is represented above or below the RL but in alternate means if first 0 is above the RL then second 0 will be below the RL the next 0 will be above the RL and so on.

Note :- It is opposite of Bipolar-AMI

Digital Value - 10011100

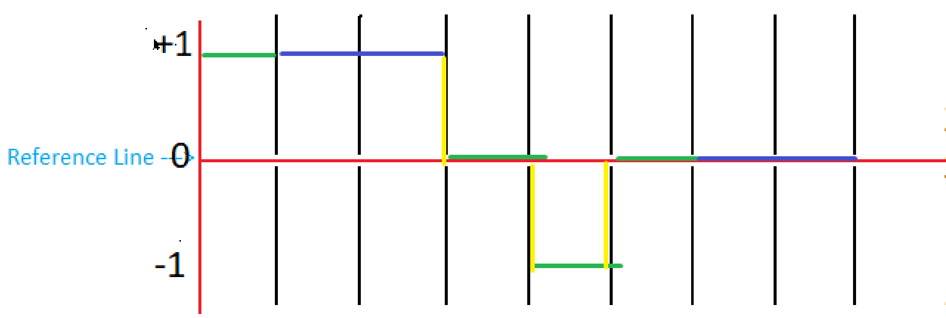
Bits	Positive	Negative
00	+1	-1
01	+3	-3
10	-1	+1
11	-3	+3



Multilevel - 2B1Q
Always start with positive then see the level of last taken value. As per the positive or negative level of last value take value from column.

Note:- Group data in two bits.

Digital Value - 10011100

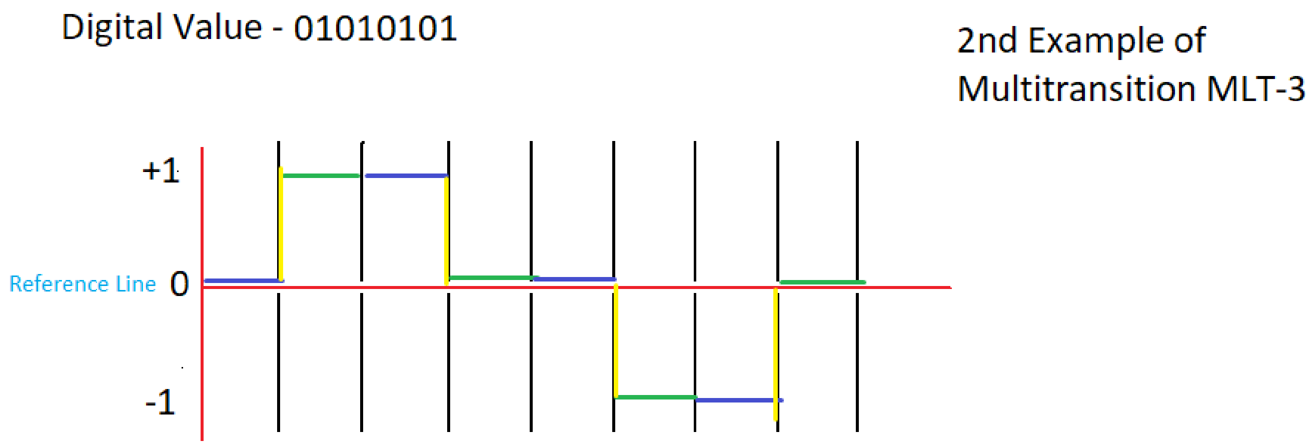


Multitransition - MLT-3
(Multi Level Transmit-3)

1. It uses 3 voltage level
   +ve, Nutral, -ve(+1,0,-1)
2. Used in telecom.
3. Generates less Ele. field

Key points for coding:

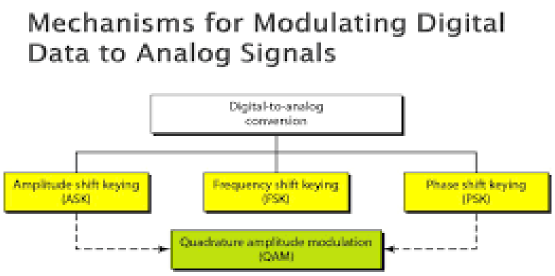
1. Very first 0 - Nutral
2. Next 0 will depend on 1 and continue 1 signal level.
3. First 1 will always +ve, second 1 nutral, 3rd 1 will be -ve, 4th 1 nutral, 5th 1 +ve, 6th 1 nutral and so on.



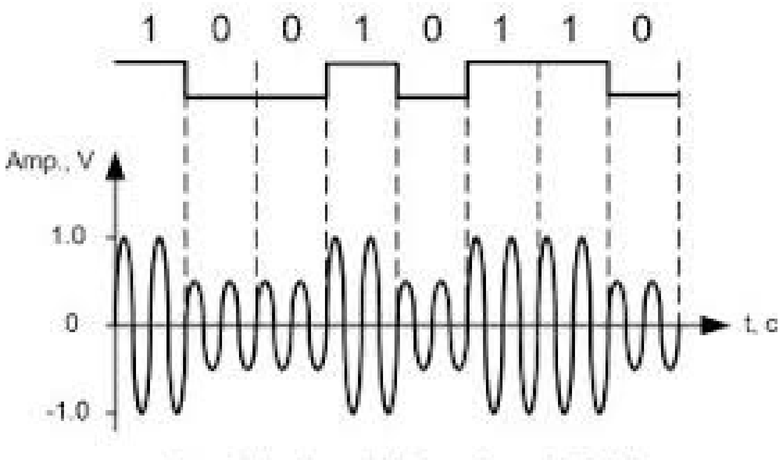
i. 1.

Digital-to-analog conversion

Digital-to-analog conversion is the process of changing one of the characteristics of an analog signal like frequency, Amplitude and phase based on the information in digital data.

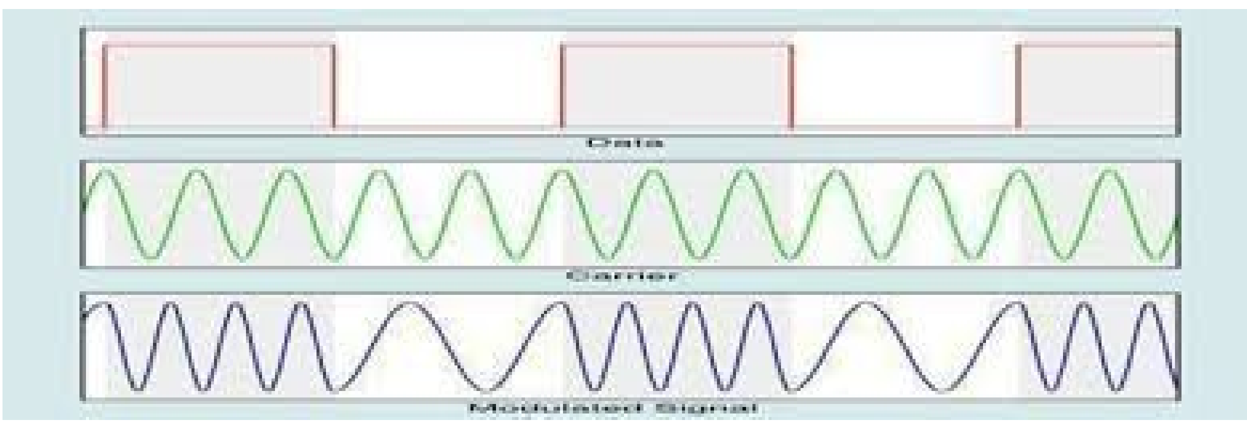


1. ASK (Amplitude Shift Keying)
In amplitude shift keying, the amplitude of the carrier signal is varied to create signal elements. Both frequency and phase remain constant while the amplitude changes.

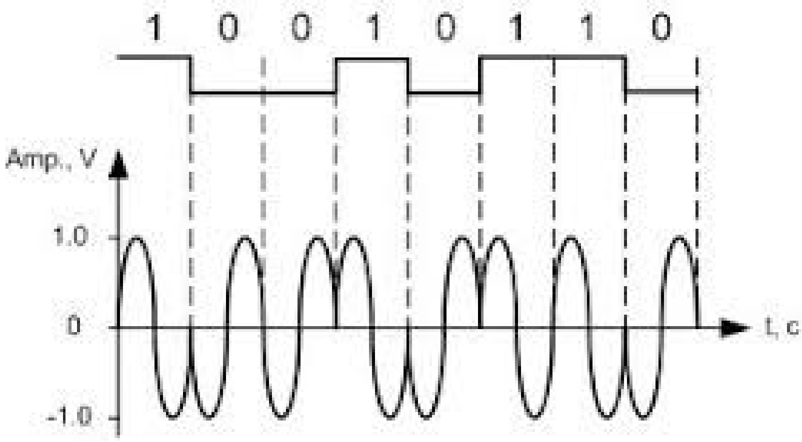


Amplitude shift keying (ASK)

2. FSK(Frequency Shift Keying)
In frequency shift keying, the frequency ofthe carrier signal is varied to represent data. The frequency of the modulated signal is constant for the duration of one signal ele- ment, but changes for the next signal element if the data element changes. Both peak amplitude and phase remain constant for all signal elements.

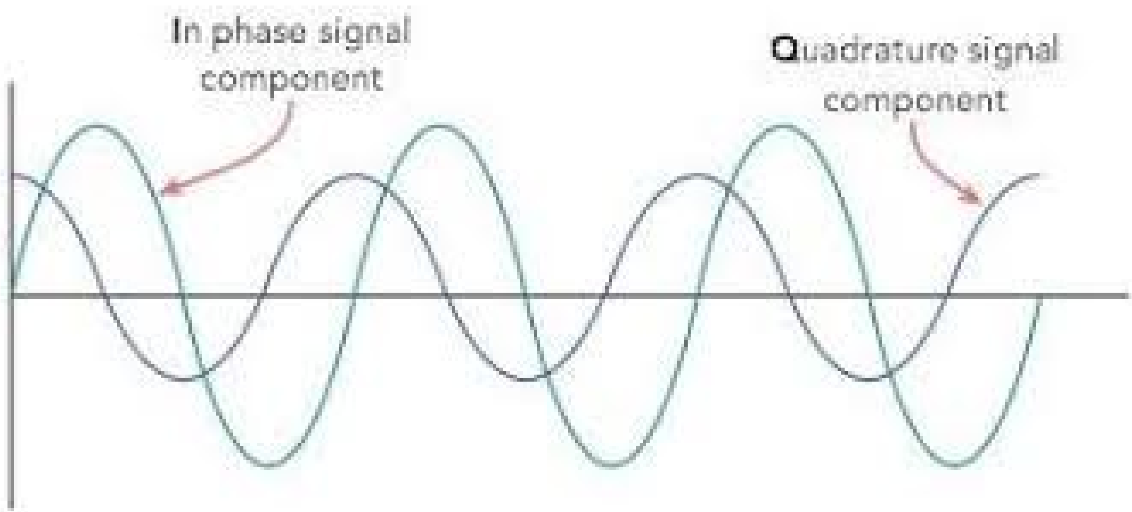


3. PSK (Phase Shift Keying)
In phase shift keying, the phase ofthe carrier is varied to represent two or more differ- ent signal elements. Both peak amplitude and frequency remain constant as the phase changes.



Phase shift keying (PSK)

4. QAM(Quadrature Amplitude Modulation)
   PSK is limited by the ability of the equipment to distinguish small differences in phase. This factor limits its potential bit rate. So far, we have been altering only one of the three characteristics of a sine wave at a time; but what if we alter two? Combination of ASK and PSK. The idea of using two carriers, one in-phase and the other quadrature, with different amplitude levels for each carrier is the concept behind quadrature amplitude modulation (QAM).

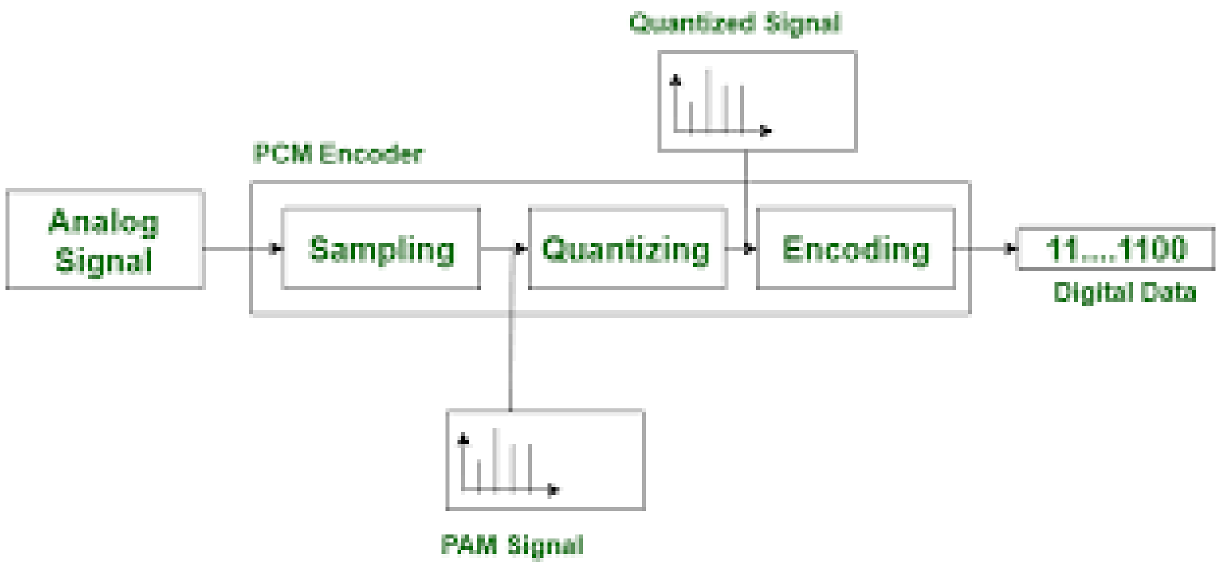


ANALOG-TO-DIGITAL CONVERSION

A process to change analog signal to digital signal is known as Pulse Code Modulation (PCM)

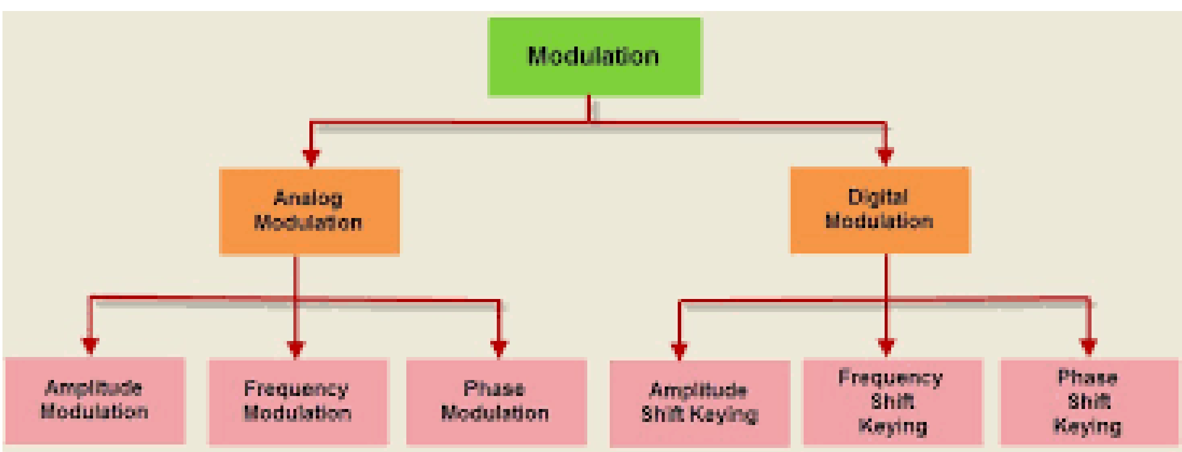
PAM & PCM

DM (Delta Modulation)
Analog Signal ---→ Sampling --→ Quantization --→ Encoding --→ Digital Signal

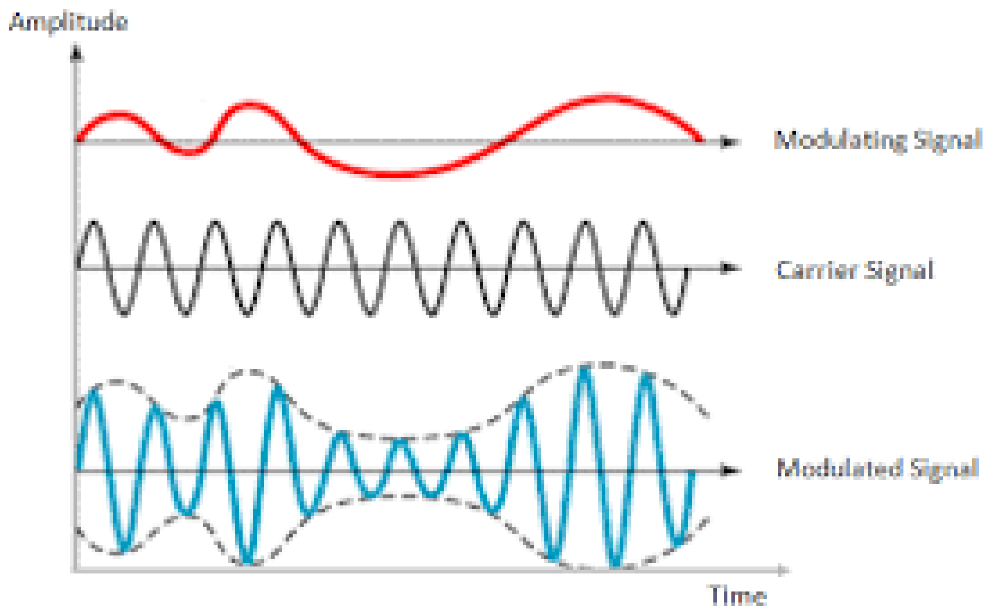


Block Diagram Of PCM

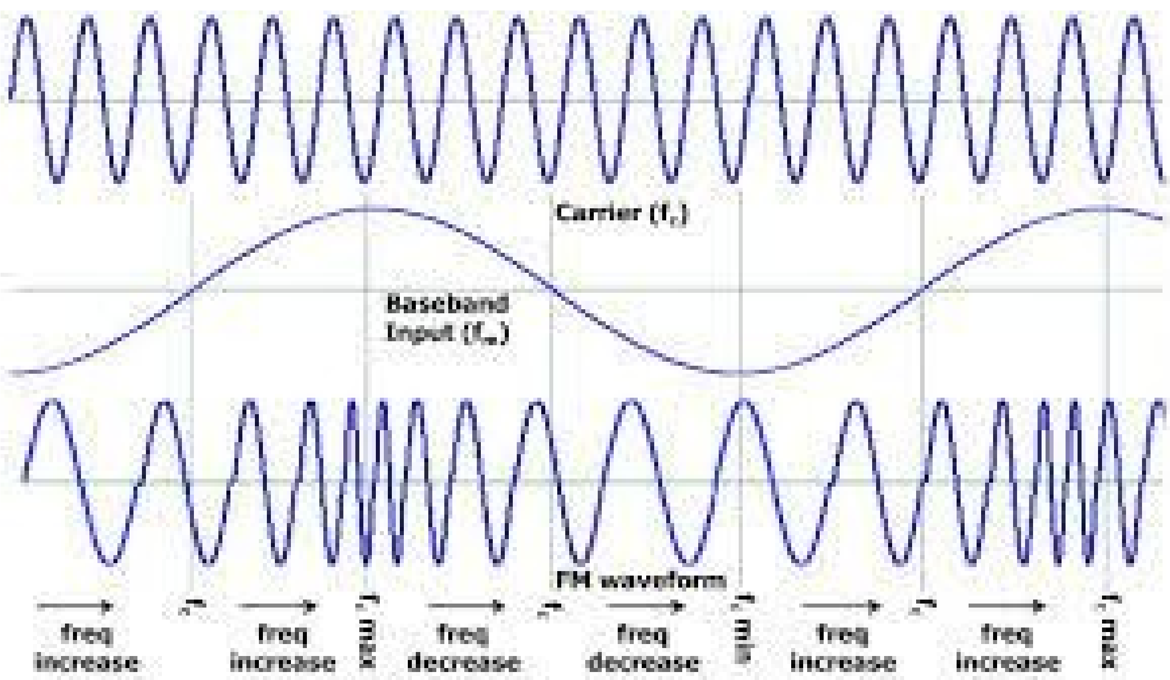
ANALOG-TO-ANALOG CONVERSION



Amplitude Modulation



Frequency Modulation



Pulse Modulation

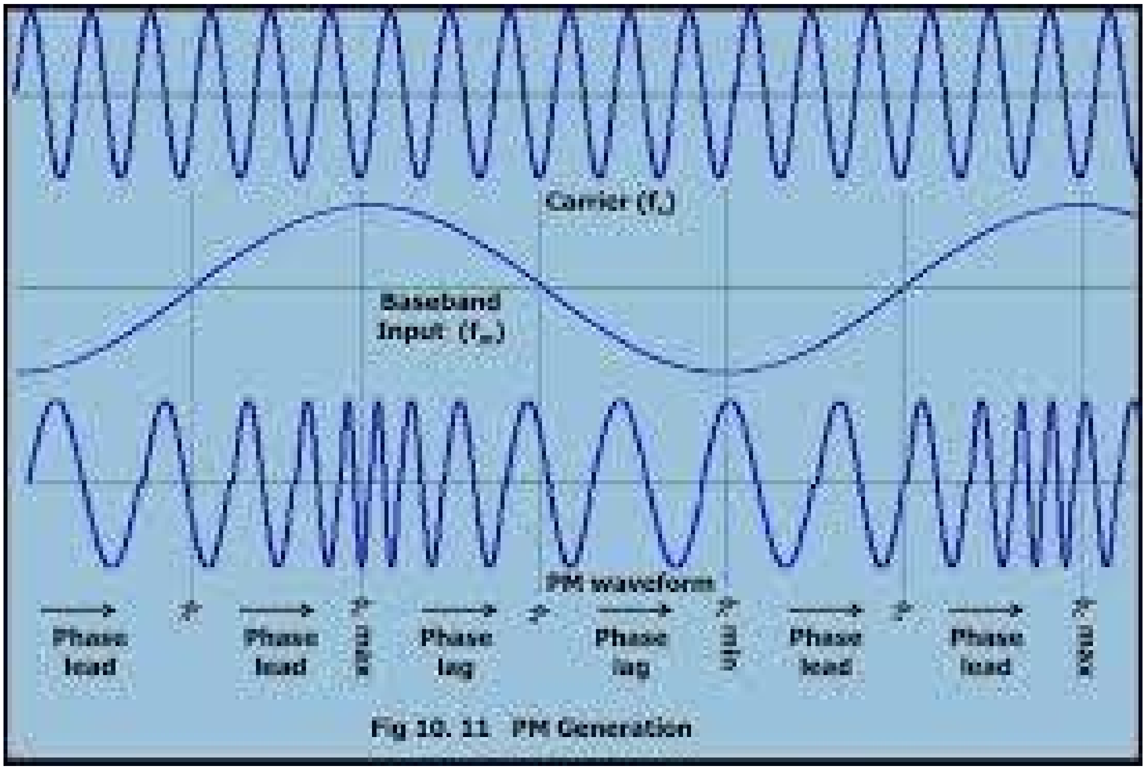


Fig 10. 11 PM Generation

Multiplexing & De-multiplexing

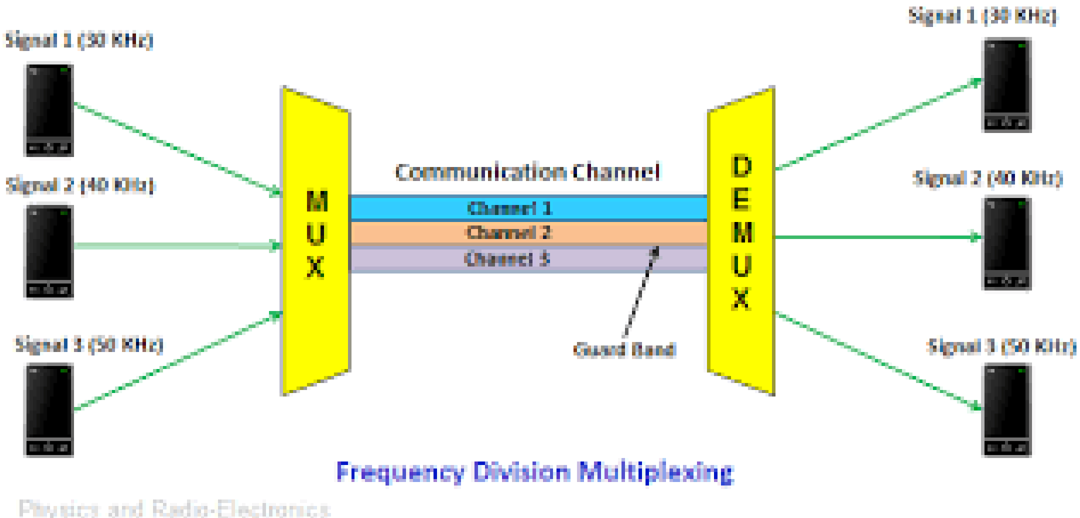
Multiplexing means combining multiple signal into single signal and **De-multiplexing** means breaking multiplexed signal into multiple signal.

Types and description:->

Frequency-Division Multiplexing

Frequency-division multiplexing (FDM) is an analog technique that can be applied when the bandwidth of a link (in hertz) is greater than the combined bandwidths of the signals to be transmitted. In FDM, signals generated by each sending device modulate different carrier frequencies. These modulated signals are then combined into a single composite signal that can be transported by the link. Carrier frequencies are separated by sufficient bandwidth to accommodate the modulated signal. These bandwidth ranges are the channels through which the various signals travel. Channels can be separated by strips of unused bandwidth-guard bands-to prevent signals from overlapping. In addition, carrier frequencies must not interfere with the original data frequencies.

Example: Radio, Television, GSM



Wavelength-Division Multiplexing

Wavelength-division multiplexing (WDM) is designed to use the high-data-rate capability of fiber optic cable. The optical fiber data rate is higher than the data rate of metallic transmission cable. Using a fiber optic cable for one single line wastes the available bandwidth. Multiplexing allows us to combine several lines into one.WDM is conceptually the same as FDM, except that the multiplexing and de-multiplexing involve optical signals transmitted through fiber optic channels. The idea is the same: We are combining different signals of different frequencies. The difference is that the frequencies are very high.

Example: Fiber Optic Cable

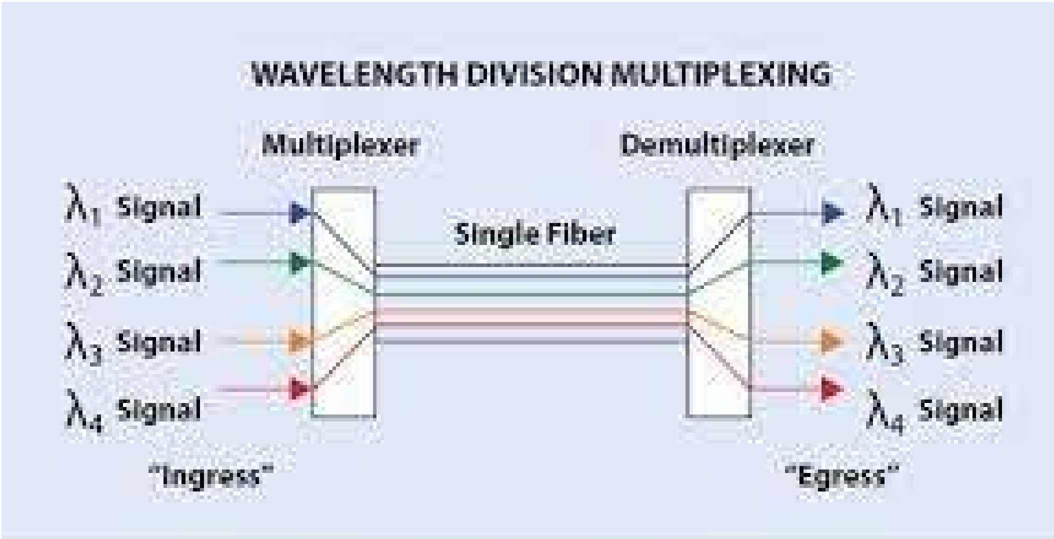
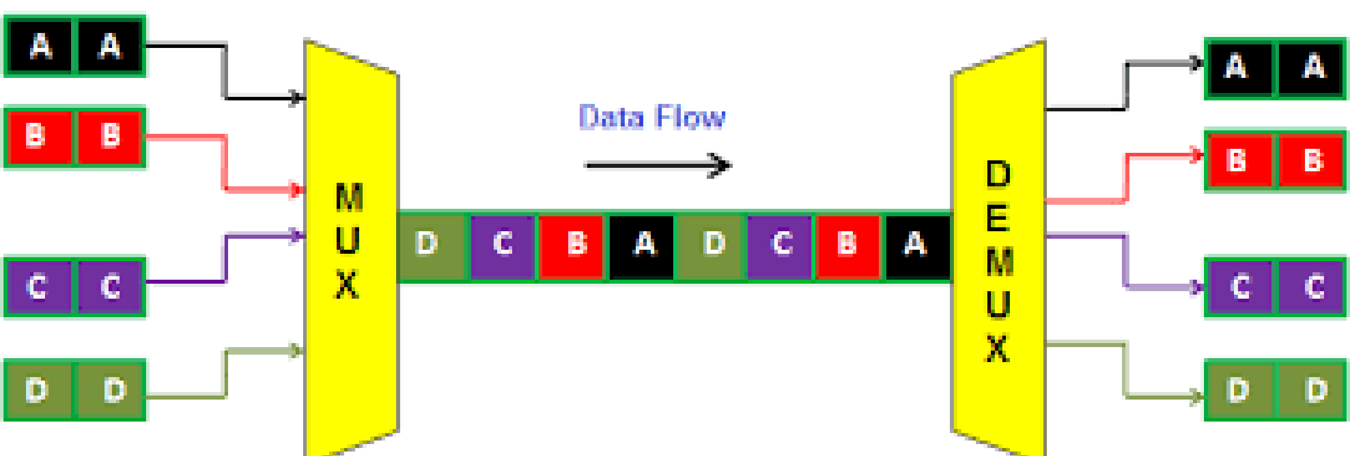


Figure 1: Basic WDM Technology Diagram

Time-devision Multiplexing

Time-division multiplexing (TDM) is a digital process that allows several connections to share the high bandwidth of a line Instead of sharing a portion of the bandwidth as in FDM, time is shared. Each connection occupies a portion of time in the link. Figure 6.12 gives a conceptual view of TDM. Note that the same link is used as in FDM; here, how- ever, the link is shown sectioned by time rather than by frequency. In the figure, portions of signals 1,2,3, and 4 occupy the link sequentially.

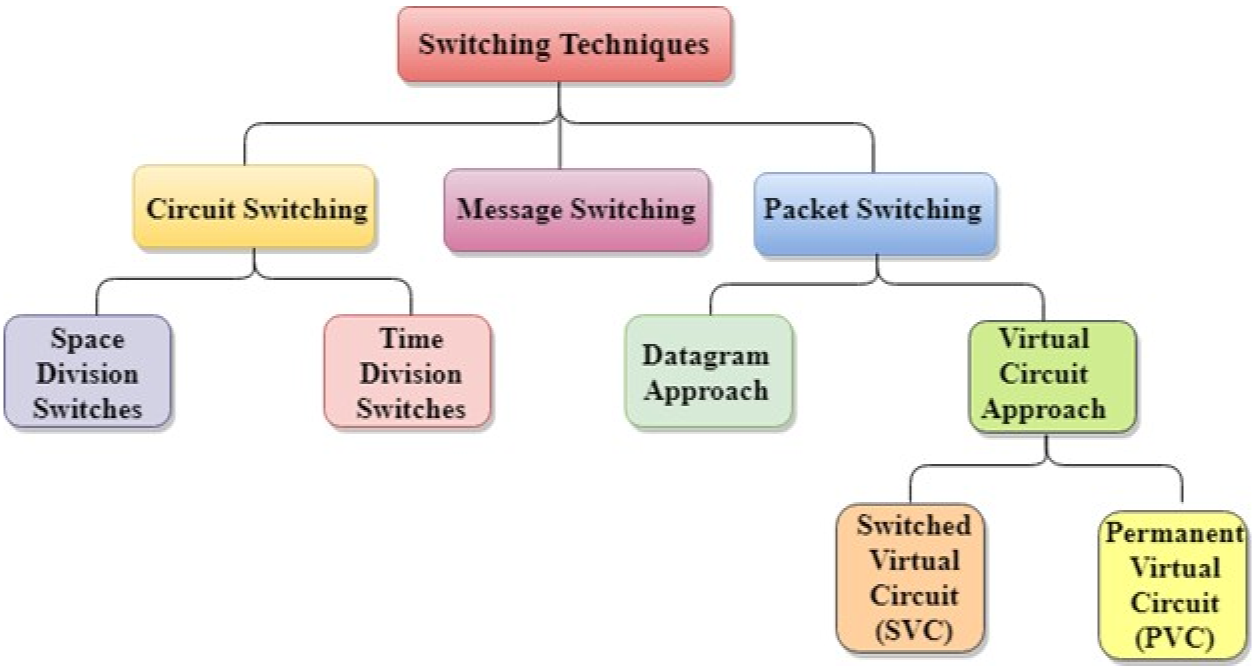
Example: GSM (Global System for Mobile Communication)



Time Division Multiplexing

Switching

Switching is the technique by which nodes control or switch data to transmit it between specific points on a network.



Circuit Switching :

In circuit switching network resources (bandwidth) are divided into channels for dedicated connection. The dedicated path/circuit established between sender and receiver provides a guaranteed data rate. Data can be transmitted without any delays once the circuit is established.

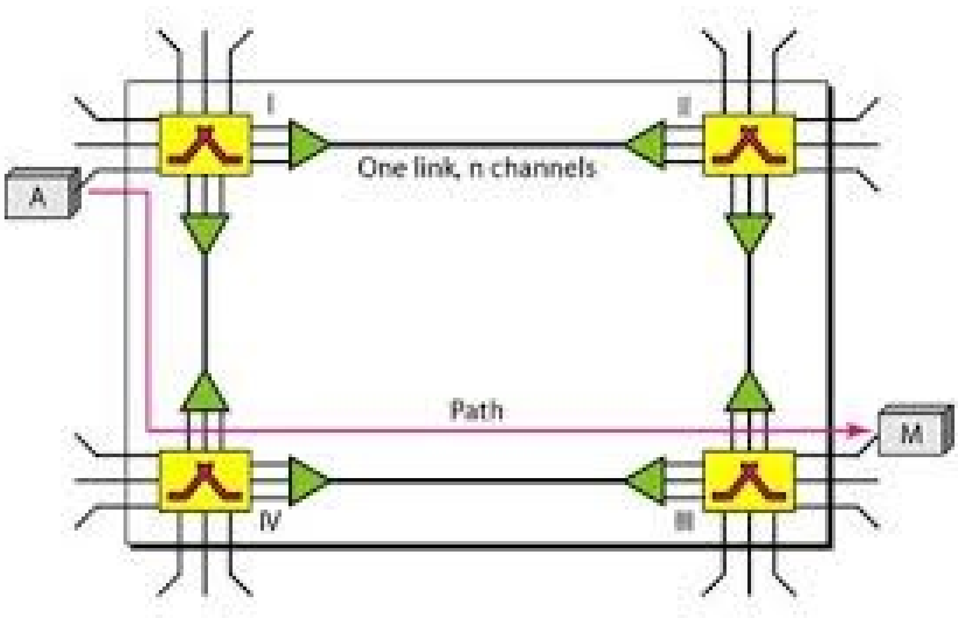
Switched based network and Telephone system network are examples of Circuit switching. **TDM (Time Division Multiplexing) and FDM (Frequency Division Multiplexing)** are two methods of multiplexing multiple signals into a single carrier.

Advantages of Circuit Switching:

1. The main advantage of circuit switching is that a committed transmission channel is established between the computers which give a guaranteed data rate.
2. In-circuit switching, there is no delay in data flow because of the dedicated transmission path.

Disadvantages of Circuit Switching:

1. It takes a long time to establish a connection.
2. More bandwidth is required in setting up dedicated channels.
3. It cannot be used to transmit any other data even if the channel is free as the connection is dedicated to circuit switching.



Packet switching

Packet switching is a method of transferring the data to a network in form of packets. In order to transfer the file fast and efficiently manner over the network and minimize the transmission latency, the data is broken into small pieces of variable length, called **Packet**. At the destination, all these small parts (packets) have to be reassembled, belonging to the same file. A packet composes of payload and various control information. No pre-setup or reservation of resources is needed. Packet Switching uses **Store and Forward** technique while switching the packets; while forwarding the packet each hop first stores that packet then forward. This technique is very beneficial because packets may get discarded at any hop due to some reason. More than one path is possible between a pair of sources and destinations. Each packet contains Source and destination address using which they independently travel through the network. In other words, packets belonging to the same file may or may not travel through the same path. If there is congestion at some path, packets are allowed to choose different paths possible over an existing network.

Advantage of Packet Switching over Circuit Switching :

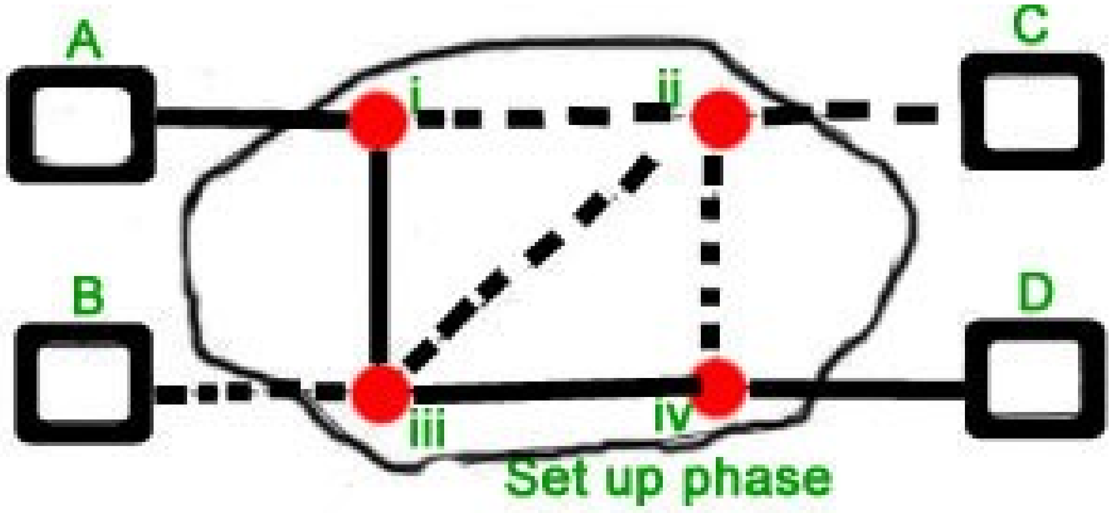
- More efficient in terms of bandwidth, since the concept of reserving circuit is not there.
- Minimal transmission latency.
- More reliable as a destination can detect the missing packet.
- More fault tolerant because packets may follow a different path in case any link is down, Unlike Circuit Switching.
- Cost-effective and comparatively cheaper to implement.

The disadvantage of Packet Switching over Circuit Switching :

- Packet Switching doesn’t give packets in order, whereas Circuit Switching provides ordered delivery of packets because all the packets follow the same path.
- Since the packets are unordered, we need to provide sequence numbers for each packet.
- Complexity is more at each node because of the facility to follow multiple paths.
- Transmission delay is more because of rerouting.
- Packet Switching is beneficial only for small messages, but for bursty data (large messages) Circuit Switching is better.

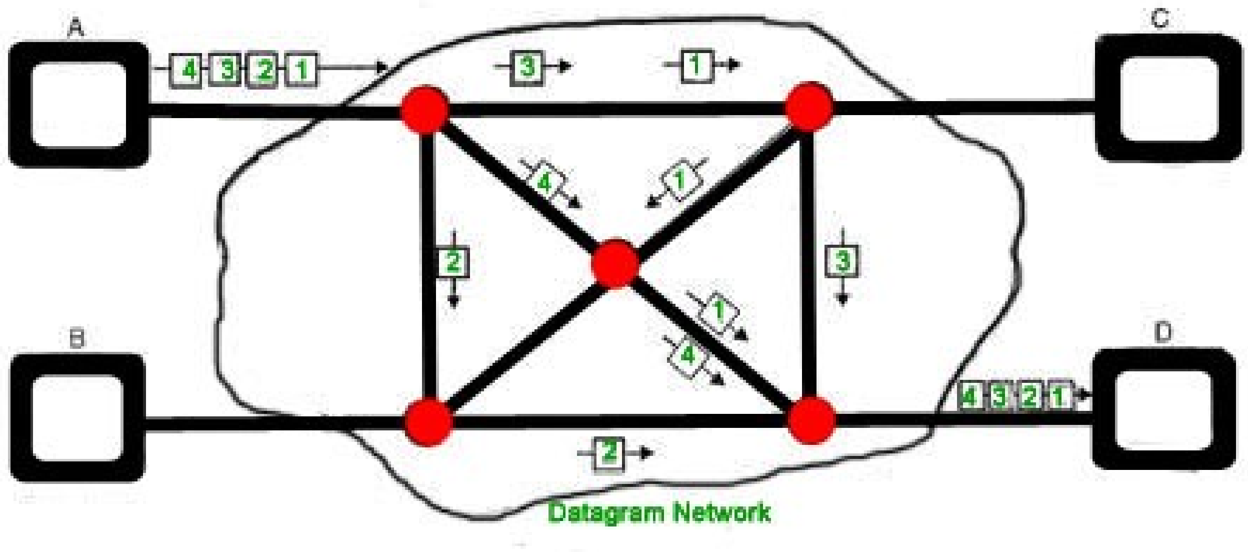
Modes of Packet Switching :

1. **Connection-oriented Packet Switching (Virtual Circuit) :** Before starting the transmission, it establishes a logical path or virtual connection using signaling protocol, between sender and receiver and all packets belongs to this flow will follow this predefined route. Virtual Circuit ID is provided by switches/routers to uniquely identify this virtual connection. Data is divided into small units and all these small units are appended with help of sequence numbers. Overall, three phases take place here- The setup, data transfer and tear down phase.



All address information is only transferred during the setup phase. Once the route to a destination is discovered, entry is added to the switching table of each intermediate node. During data transfer, packet header (local header) may contain information such as length, timestamp, sequence number, etc.
Connection-oriented switching is very useful in switched WAN. Some popular protocols which use the Virtual Circuit Switching approach are X.25, Frame-Relay, ATM, and MPLS(Multi-Protocol Label Switching).

2. **Connectionless Packet Switching (Datagram) :**
   Unlike Connection-oriented packet switching, In Connectionless Packet Switching each packet contains all necessary addressing information such as source address, destination address and port numbers, etc. In Datagram Packet Switching, each packet is treated independently. Packets belonging to one flow may take different routes because routing decisions are made dynamically, so the packets arrived at the destination might be out of order. It has no connection setup and teardown phase, like Virtual Circuits.
   Packet delivery is not guaranteed in connectionless packet switching, so reliable delivery must be provided by end systems using additional protocols.



Datagram Packet Switching

Message Switching –

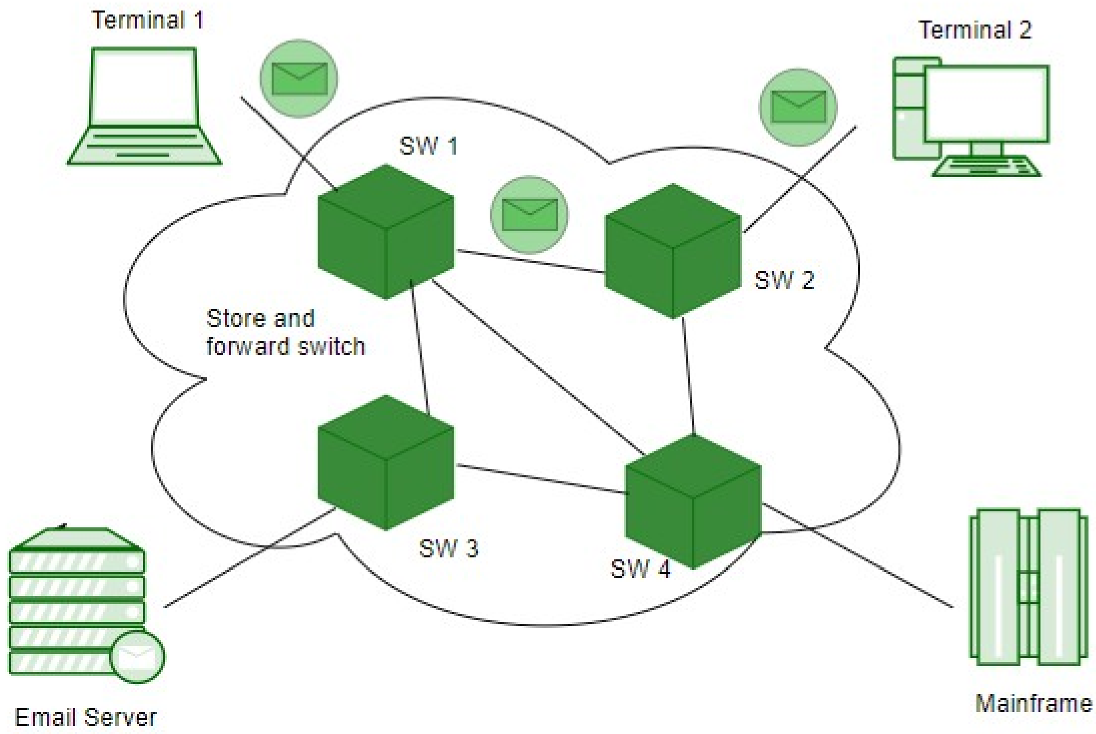
Message switching was a technique developed as an alternative to circuit switching before packet switching was introduced. In message switching, end-users communicate by sending and receiving *messages* that included the entire data to be shared. Messages are the smallest individual unit. Also, the sender and receiver are not directly connected. There are a number of intermediate nodes that transfer data and ensure that the message reaches its destination. Message switched data networks are hence called hop-by-hop systems.

They provide 2 distinct and important characteristics:

1. **Store and forward –** The intermediate nodes have the responsibility of transferring the entire message to the next node. Hence, each node must have storage capacity. A message will only be delivered if the next hop and the link connecting it are both available, otherwise, it'll be stored indefinitely. A store-and-forward switch forwards a message only if sufficient resources are available and the next hop is accepting data. This is called the store-and-forward property.

2. **Message delivery –** This implies wrapping the entire information in a single message and transferring it from the source to the destination node. Each message must have a header that contains the message routing information, including the source and destination.

Message switching network consists of transmission links (channels), store-and-forward switch nodes, and end stations as shown in the following picture:



Characteristics of message switching –
Message switching is advantageous as it enables efficient usage of network resources. Also, because of the store-and-forward capability of intermediary nodes, traffic can be efficiently regulated and controlled. Message delivery as one unit, rather than in pieces, is another benefit. However, message switching has certain disadvantages as well. Since messages are stored indefinitely at each intermediate node, switches require a large storage capacity. Also, these are pretty slow. This is because at each node, first there is a wait till the entire message is received, then it must be stored and transmitted after processing the next node and links to it depending on availability and channel traffic. Hence, message switching cannot be used for real-time or interactive applications like a video conference.

Advantages of Message Switching –
Message switching has the following advantages:

1. As message switching is able to store the message for which communication channel is not available, it helps in reducing the traffic congestion in the network.
2. In message switching, the data channels are shared by the network devices.

3. It makes traffic management efficient by assigning priorities to the messages.

Disadvantages of Message Switching –

Message switching has the following disadvantages:

1. Message switching cannot be used for real-time applications as storing messages causes delay.
2. In message switching, the message has to be stored for which every intermediate device in the network requires a large storing capacity.

Applications –

The store-and-forward method was implemented in telegraph message switching centers. Today, although many major networks and systems are packet-switched or circuit-switched networks, their delivery processes can be based on message switching. For example, in most electronic mail systems the delivery process is based on message switching, while the network is in fact either circuit-switched or packet-switched.

Telephone Network:

Telephone networks use circuit switching. The telephone network had its beginnings in the late 1800s. The entire network, which is referred to as the plain old telephone system (POTS), was originally an analog system using analog signals to transmit voice. With the advent of the computer era, the

network, in the 1980s, began to carry data in addition to voice. During the last decade, the telephone network has undergone many technical changes. The network is now digital as well as analog.

Dialup Modem

The term modem is a composite word that refers to the two functional entities that make up the device: a signal modulator and a signal demodulator. A modulator creates analog signal from binary data. A demodulator recovers the binary data from the modulated signal.

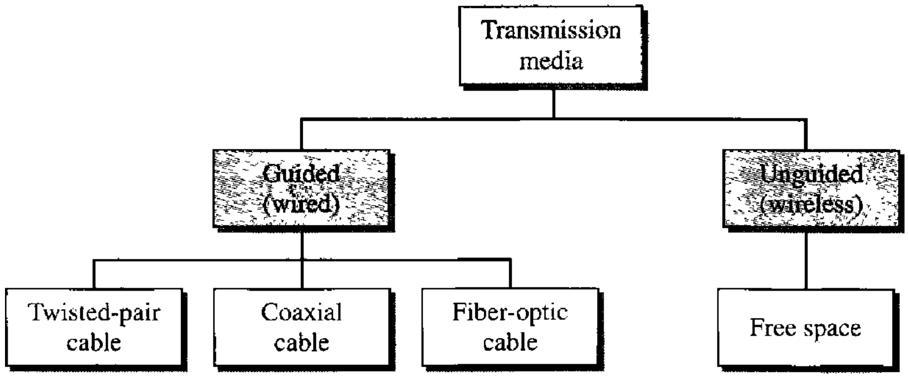
Digital Subscriber Line (DSL)

After traditional modems reached their peak data rate, telephone companies developed another technology, DSL, to provide higher-speed access to the Internet. Digital subscriber line (DSL) technology is one of the most promising for supporting high-speed digital communication over the existing local loops. DSL technology is a set of technologies, each differing in the first letter (ADSL, VDSL, HDSL, and SDSL). The set is often referred to as xDSL, where x can be replaced by A, V, H, or S.

Technology	downstream	Upstream	Distance(ft)	Twisted Pair	Line Coding
ADSL	**1.5-6.1 Mbps**	**16-640 kbps**	**12000**	**1**	**DMT**
HDSL	**1.5-2.0 Mbps**	**1.5-2.0 Mbps**	**12000**	**2**	**2B1Q**
SDSL	**768 kbps**	**768 kbps**	**12000**	**1**	**2B1Q**
VDSL	**25-55 Mbps**	**3.2 Mbps**	**3000-10000**	**1**	**DMT**

Transmission Media:

A transmission **medium / media** can be broadly defined as anything that can carry information from a source to a destination.

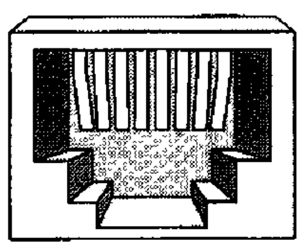


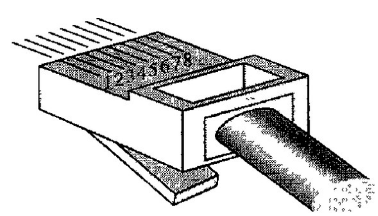
Guided Media :

Guided media, which are those that provide a conduit from one device to another,
include twisted-pair cable, coaxial cable, and fiber-optic cable. A signal traveling
along any of these media is directed and contained by the physical limits of the medium.

Twisted Pair Cable:

1. Metallic cable with plastic cover is used.
2. Cables are twisted in pairs to avoid distortion of signal.
3.Distance Coverage - up to 100m
4. Connector - RJ-45 with 8 pins, RJ-11 with 4 pins


RJ-45 Female


RJ-45 Male

5. Used in star topology based network, Telephone line, Internet Service.
6. Speed into Gbps.
7. Categories - Cat 1, Cat 2, Cat 3, Cat 4, Cat 5, Cat 5e, Cat 6, Cat 7
8. Types : Shielded Twisted Pair (STP)
   Unshielded Twisted Pair (UTP)
9. STP - It has very less effect of EMI.
   Mostly used in external part of network.

10. UTP - It has more effect of EMI than STP.
Mostly used in internal part of network.

TIA/EIA standard

568A

WG
G
WO
B
WB
O
WBr
Br

568B

WO
O
WG
B
WB
G
WBr
Br

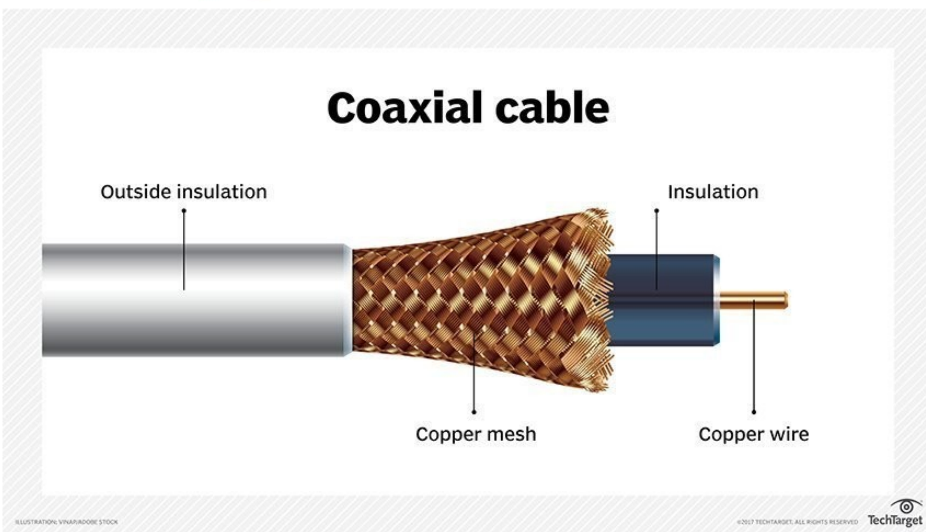
Straight Over Cable:
Used to connect a node with Switch, Router to Switch, Switch to printer
Notes:-> Any one standard can be used at both end of a cable.

Cross Over Cable
Used to connect similar devices like router to router, Switch to switch, PC to PC, Laptop to Laptop.
Notes: -> Use both standard means if at one end 568A then at second end 568B.

Roll Over Cable
Used to configure devices like router, switch

Coaxial Cable:

1. Single Metallic cable with plastic cover is used.
2. Copper Mesh is used to protect the data signal from distortion.
3. Used to connect TV set with satellite and Bus Topology based Network.
4. Distance Coverage = up to 500m
5. Data Transfer rate = up to 10mbps
6. Connector = BNC (Bayone-Neill-Concelman)



7. Types :

   a. RG58 - 10Base2- Thin Coaxial Cable

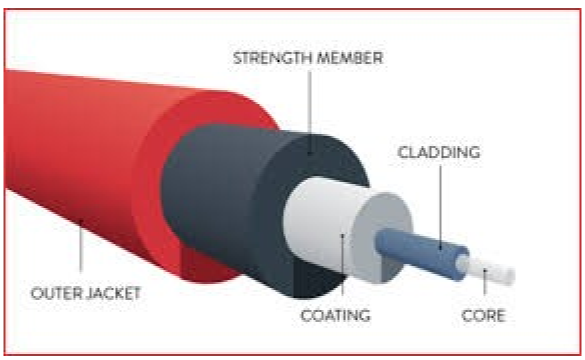
Thin coaxial cable is also referred to as thinnet. 10Base2 refers to the specifications for **thin coaxial cable** carrying Ethernet signals. The 2 refers to the approximate maximum segment length being 200 meters. In actual fact the maximum segment length is 185 meters.

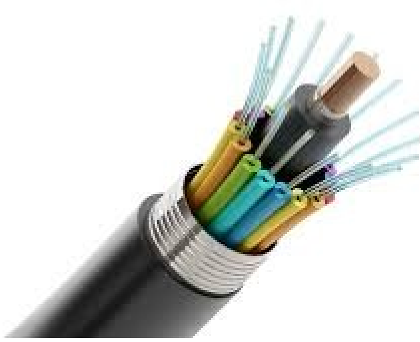
   b. RG8 - 10Base5 - Thick Coaxial Cable

Thick coaxial cable is also referred to as thicknet. 10Base5 refers to the specifications for **thick coaxial cable** carrying Ethernet signals. The 5 refers to the maximum segment length being 500 meters. **Thick coaxial cable** has an extra protective plastic cover that helps keep moisture away from the center conductor.

Fiber Optic Cable / Optical Fiber Cable (OFC)

1. Data is transferred in the form of light.
2. Fiber or glass is used as medium for data transmission.
3. It works at total internal reflection.
4. No effect of electromagnetic field.
5. Distance coverage = up to 10km
6. Connector = SC(**subscriber channel), ST (Straight Tip), MT-RJ**
7. **Few Types On the basis of Speed and distance:**
    a. **100Base-FX -> Speed 100 Mbps , distance up to 2 Km**
    b. **1000Base - FX** -> Speed 1000 Mbps , distance up to 550m
8. Types on the basis of signal carried at a time :
    a. Single Mode : On signal at a time.
    b. Multimode : Multiple Signal At a time.





SC Connector

ST Connector

MT-RJ

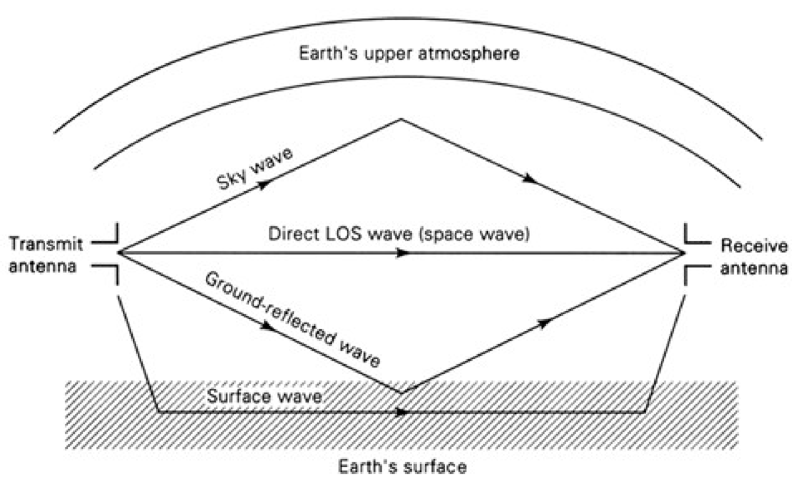
SMA

Unguided Media :

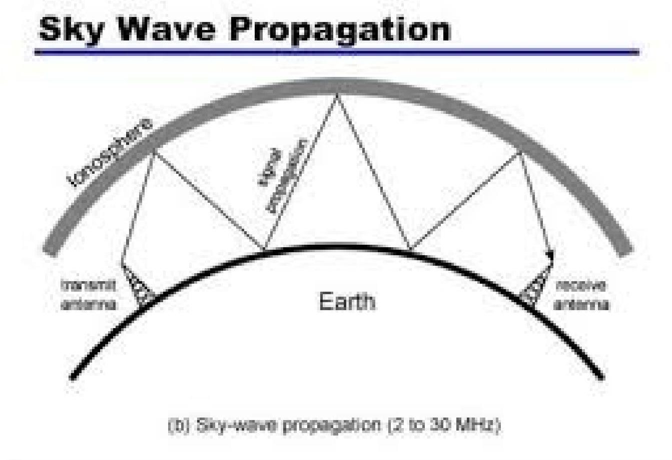
1. It uses free space.
2. Transmission is done using frequency(Electromagnetic Waves). This is also known as Wireless Transmission.
3. It provides portability in infrastructure.

Ways to transmit waves :

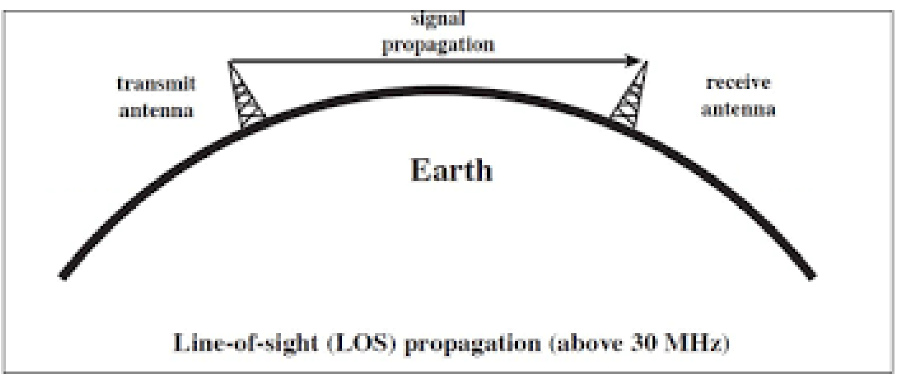
1. Ground Propagation - Radio waves travel through the lowest portion of the atmosphere, hugging the earth. These low-frequency signals emanate in all directions from the transmitting antenna and follow the curvature of the planet. Distance depends on the amount of power in the signal: The greater the power, the greater the distance.



2. Sky Propagation - In this propagation, higher-frequency radio waves radiate upward into the ionosphere(the layer of atmosphere where particles exist as ions) where they are reflected back toearth. This type of transmission allows for greater distances with lower output power.



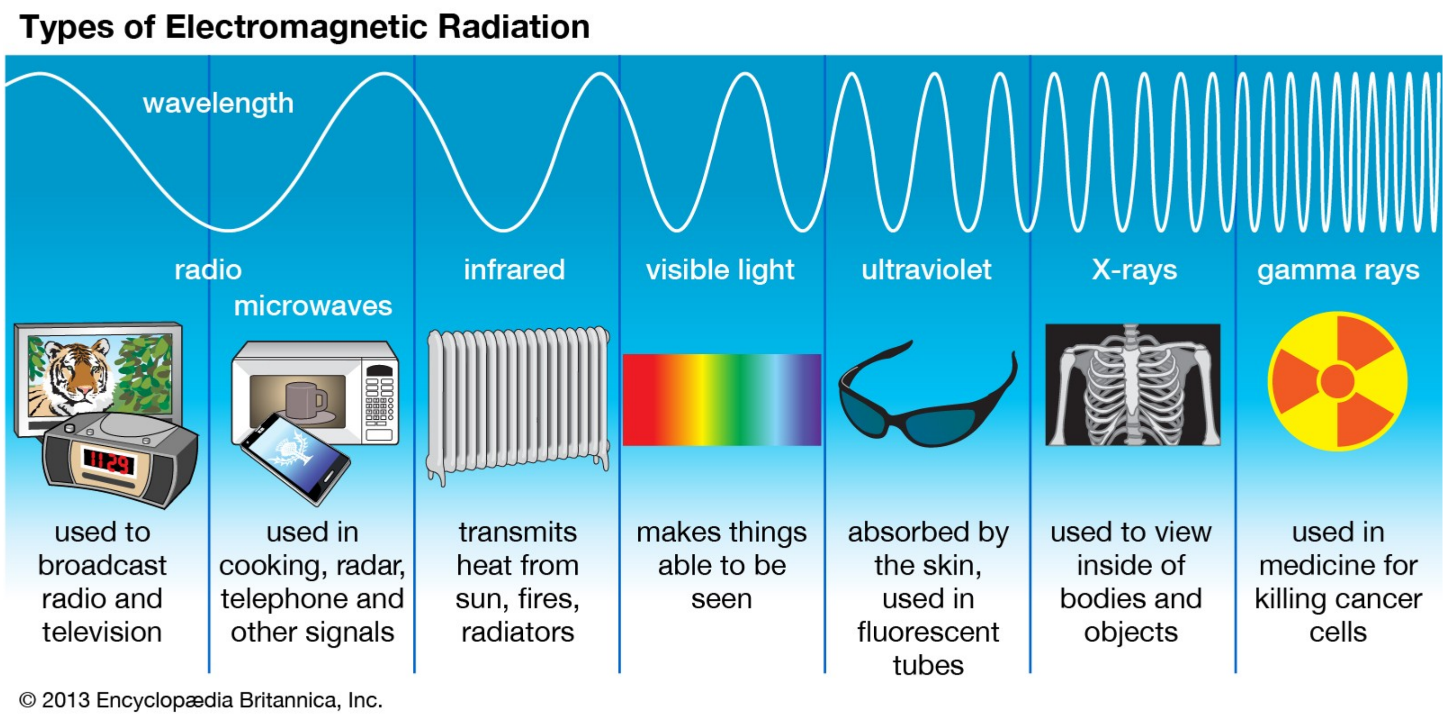
3. Line of Sight Propagation - very high-frequency signals are transmitted in straight lines directly from antenna to antenna. Antennas must be directional, facing each other, and either tall enough or close enough together not to be affected by the curvature of the earth. Line-of-sight propagation is tricky because radio transmissions cannot be completely focused.



Class			Freq-uency
Ionizing radiation	γ	Gamma rays	300 EHz
			30 EHz

	HX	Hard X-rays	
			3 EHz
	SX	Soft X-rays	300 PHz
			30 PHz
	EUV	Extreme ultraviolet	
			3 PHz
	NUV	Near ultraviolet, visible	
			300 THz
	NIR	Near infrared	
			30 THz
	MIR	Mid infrared	
			3 THz
	FIR	Far infrared	
			300 GHz
Micro-waves and radio waves	EHF	Extremely high frequency	
			30 GHz
	SHF	Super high frequency	
			3 GHz
	UHF	Ultra high frequency	
			300 MH

			z
	VHF	Very high frequency	30 MHz
	HF	High frequency	3 MHz
	MF	Medium frequency	300 kHz
	LF	Low frequency	30 kHz
	VLF	Very low frequency	3 kHz
	ULF	Ultra low frequency	300 Hz
	SLF	Super low frequency	30 Hz
	ELF	Extremely low frequency	3 Hz



Switching

A better solution is switching. A switched network consists of a series of interlinked nodes, called switches. Switches are devices capable of creating temporary connections between two or more devices linked to the switch. In a switched network, some of these nodes are connected to the end systems (computers or telephones, for example). Others are used only for routing.

In circuit switching network resources (bandwidth) are divided into pieces and bit delay is constant during a connection. The dedicated path/circuit established between sender and receiver provides a guaranteed data rate. Data can be transmitted without any delays once the circuit is established.

Telephone system network is one of the example of Circuit switching. **TDM (Time Division Multiplexing) and FDM (Frequency Division Multiplexing)** are two methods of multiplexing multiple signals into a single carrier.
Advantages of Circuit Switching:
It has the following advantages :

1. The main advantage of circuit switching is that a committed transmission channel is established between the computers which give a guaranteed data rate.
2. In-circuit switching, there is no delay in data flow because of the dedicated transmission path.

Disadvantages of Circuit Switching:

It has the following disadvantages :

1. It takes a long time to establish a connection.
2. More bandwidth is required in setting up dedicated channels.
3. It cannot be used to transmit any other data even if the channel is free as the connection is dedicated to circuit switching.

Data Link Layer:

Data link layer corrects errors which can occur at the physical layer. The layer allows you to define the protocol to establish and terminates a connection between two connected network devices.

It is IP address understandable layer, which helps you to define logical addressing so that any endpoint should be identified.

The layer also helps you implement routing of packets through a network. It helps you to define the best path, which allows you to take data from the source to the destination.

The data link layer is subdivided into two types of sub-layers:

1. Media Access Control (MAC) layer- It is responsible for controlling how device in a network gain access to medium and permits to transmit data.
2. Logical link control layer- This layer is responsible for identity and encapsulating network-layer protocols and allows you to find the error.

Important Functions of Data Link Layer:

- Framing which divides the data from Network layer into frames.
- Allows you to add header to the frame to define the physical address of the source and the destination machine
- Adds Logical addresses of the sender and receivers
- It is also responsible for the sourcing process to the destination process delivery of the entire message.

- It also offers a system for error control in which it detects retransmits damage or lost frames.
- Datalink layer also provides a mechanism to transmit data over independent networks which are linked together.

Few Important Points :

a. Framing
b. Physical addressing
c. Error control
d. Error correction
e. Data Link Control
f. Media Access control

What is framing?

Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. Ethernet, token ring, frame relay, and other data link layer technologies have their own frame structures. Frames have headers that contain information such as error-checking codes.

Ethernet (IEEE 802.3) Frame Format –

PREAMBLE	SFD	DESTINATION ADDRESS	SOURCE ADDRESS	LENGTH	DATA	CRC
7 Bytes	1 Byte	6 Bytes	6 Bytes	2 Bytes	46 - 1500 Bytes	4 Bytes

IEEE 802.3 ETHERNET Frame Format

- **PREAMBLE –** Ethernet frame starts with 7-Bytes Preamble. This is a pattern of alternative 0's and 1's which indicates starting of the frame and allow sender and receiver to establish bit synchronization. Initially, PRE (Preamble) was introduced to allow for the loss of a few bits due to signal delays. But today's high-speed Ethernet don't need Preamble to protect the frame bits.
  PRE (Preamble) indicates the receiver that frame is coming and allow the receiver to lock onto the data stream before the actual frame begins.

- **Start of frame delimiter (SFD) –** This is a 1-Byte field which is always set to 10101011. SFD indicates that upcoming bits are starting of the frame, which is the destination address. Sometimes SFD is considered the part of PRE, this is the reason Preamble is described as 8 Bytes in many places. The SFD warns station or stations that this is the last chance for synchronization.
- **Destination Address –** This is 6-Byte field which contains the MAC address of machine for which data is destined.
- **Source Address –** This is a 6-Byte field which contains the MAC address of source machine. As Source Address is always an individual address (Unicast), the least significant bit of first byte is always 0.
- **Length –** Length is a 2-Byte field, which indicates the length of entire Ethernet frame. This 16-bit field can hold the length value between 0 to 65534, but length cannot be larger than 1500 because of some own limitations of Ethernet.
- **Data –** This is the place where actual data is inserted, also known as **Payload**. Both IP header and data will be inserted here if Internet Protocol is used over Ethernet. The maximum data present may be as long as 1500 Bytes. In case data length is less than minimum length i.e. 46 bytes, then padding 0's is added to meet the minimum possible length.
- **Cyclic Redundancy Check (CRC) –** CRC is 4 Byte field. This field contains a 32-bits hash code of data, which is generated over the Destination Address, Source Address, Length, and Data field. If the checksum computed by destination is not the same as sent checksum value, data received is corrupted.

Note – Size of frame of Ethernet IEEE 802.3 varies 64 bytes to 1518 bytes including data length (46 to 1500 bytes).

Error Control

During the transmission of data, there are possibilities that data may be corrupt. So, error must be detected and corrected.

Error can be of two type:

a. Single bit error
b. Burst bits error

Error Detection - To detect error, some extra bits are added to data frames that is calculated by checksum value.

Error Correction –

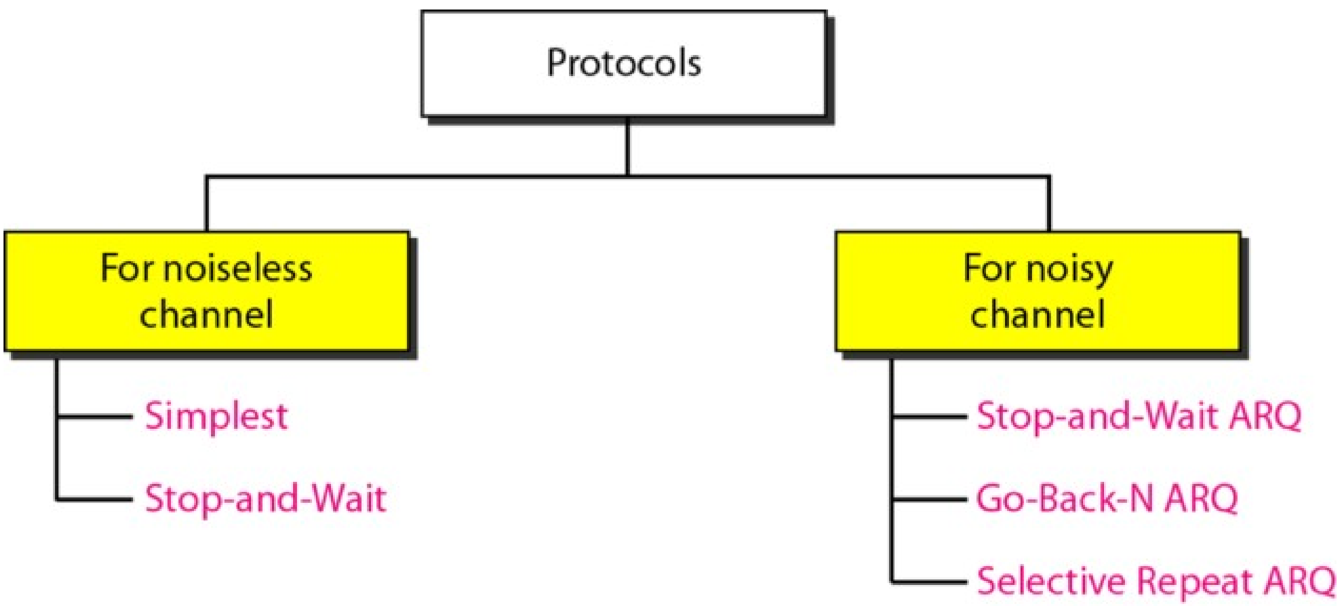
There are two main methods of error correction-

Forward error correction - It is the process in which the receiver tries to guess the message by using redundant bits. This is possible, if the number of errors is small.

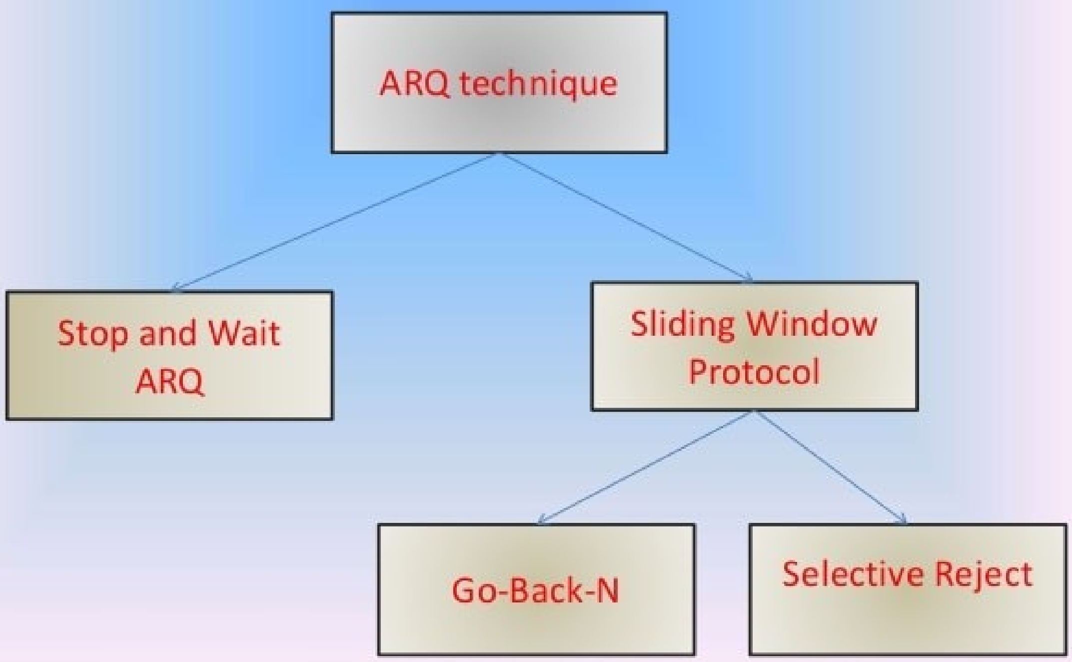
Correction by retransmission - It is a technique in which the receiver detects the occurrence of an error and asks the sender to resend the message. Resending is repeated until a message arrives that the receiver believes is error-free.

Data Link Control –

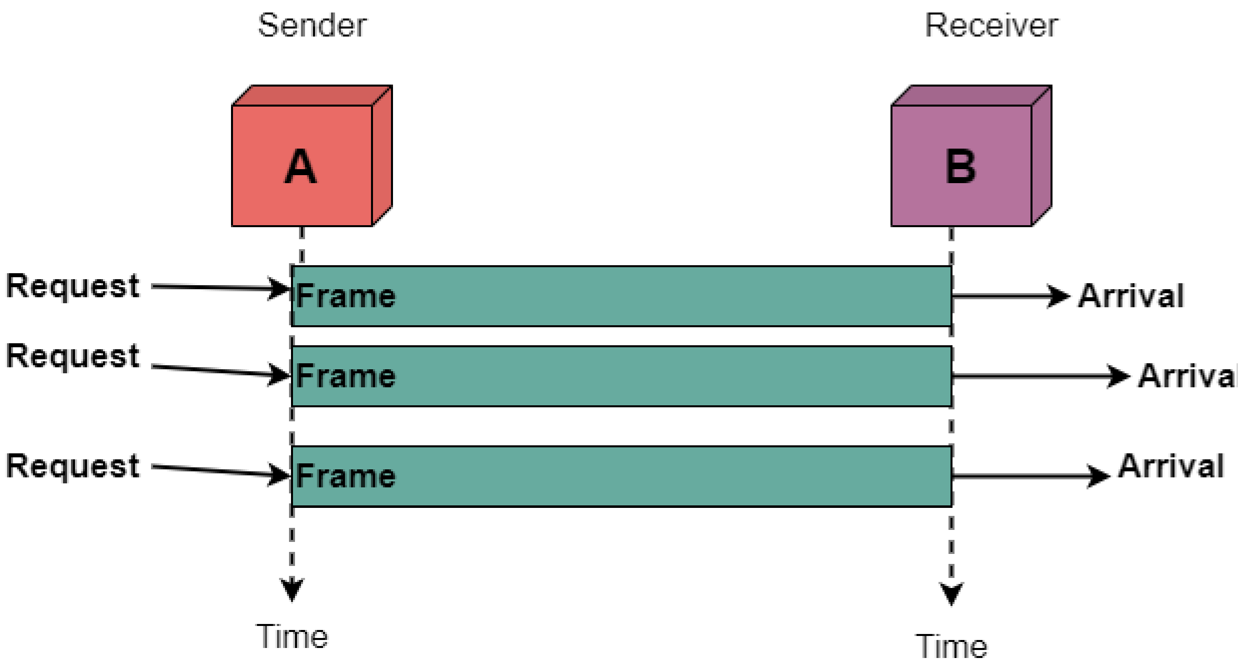
To control the link for data flow, few techniques are used by different protocols. These techniques are divided into two types :



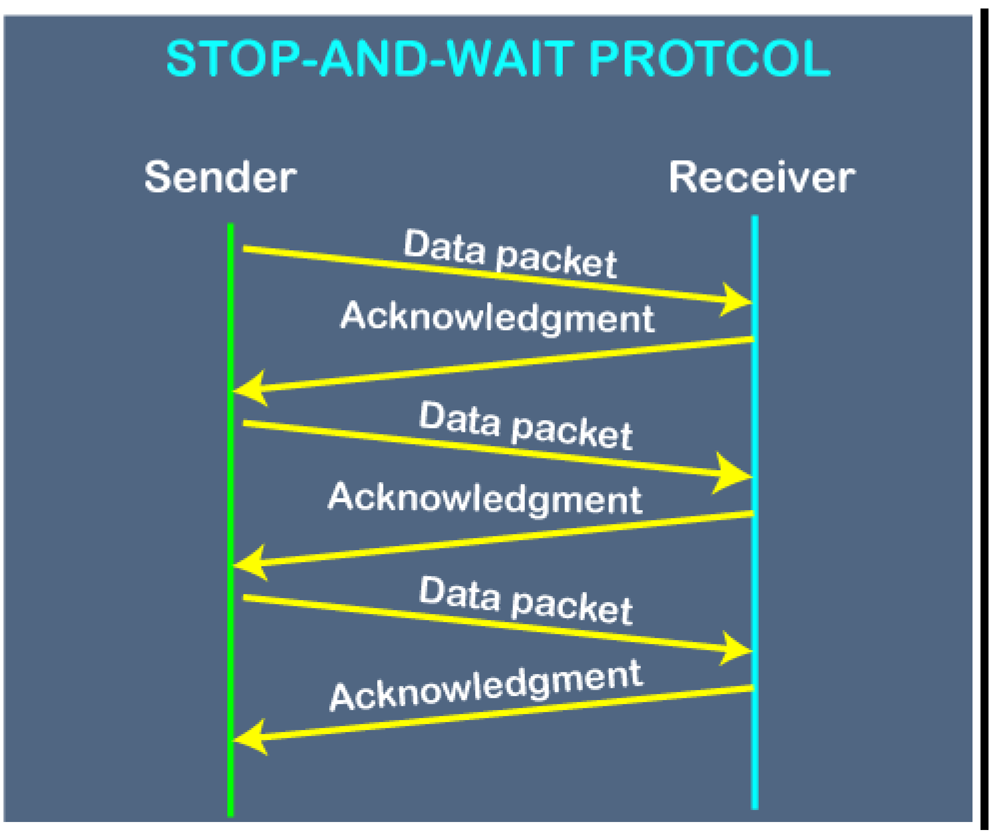
Types of ARQ...


ARQ technique
Stop and Wait ARQ
Sliding Window Protocol
Go-Back-N
Selective Reject

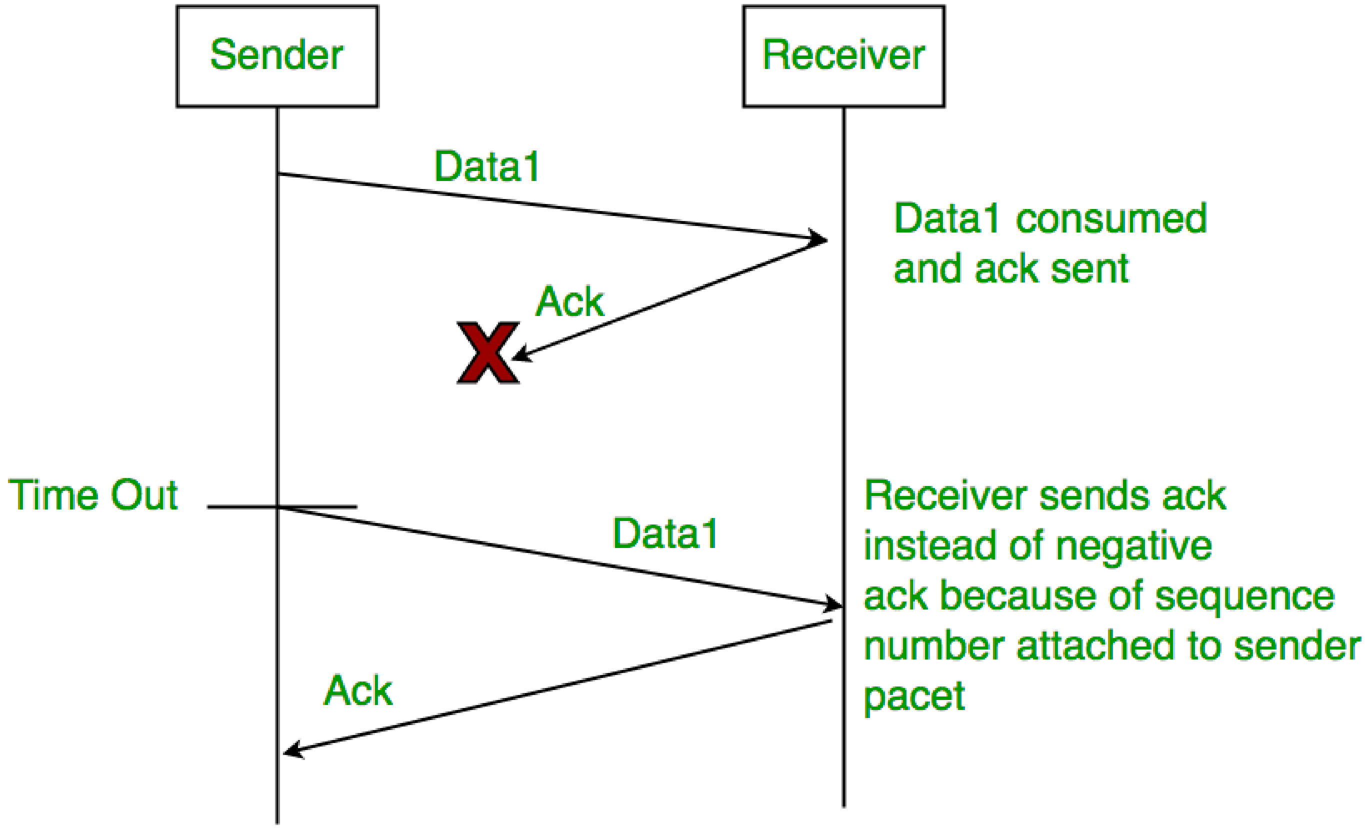
Simplest –



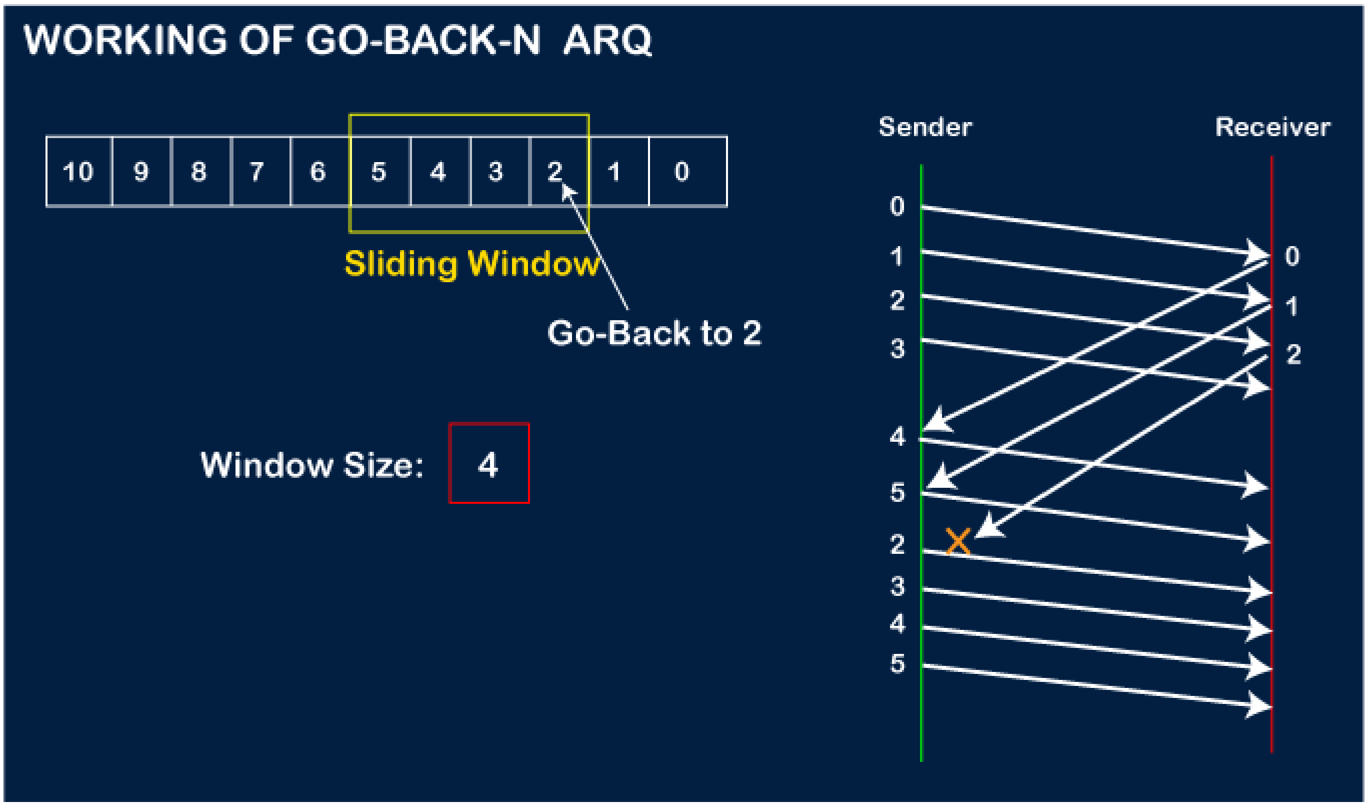
Stop and Wait –



Stop and Wait ARQ –

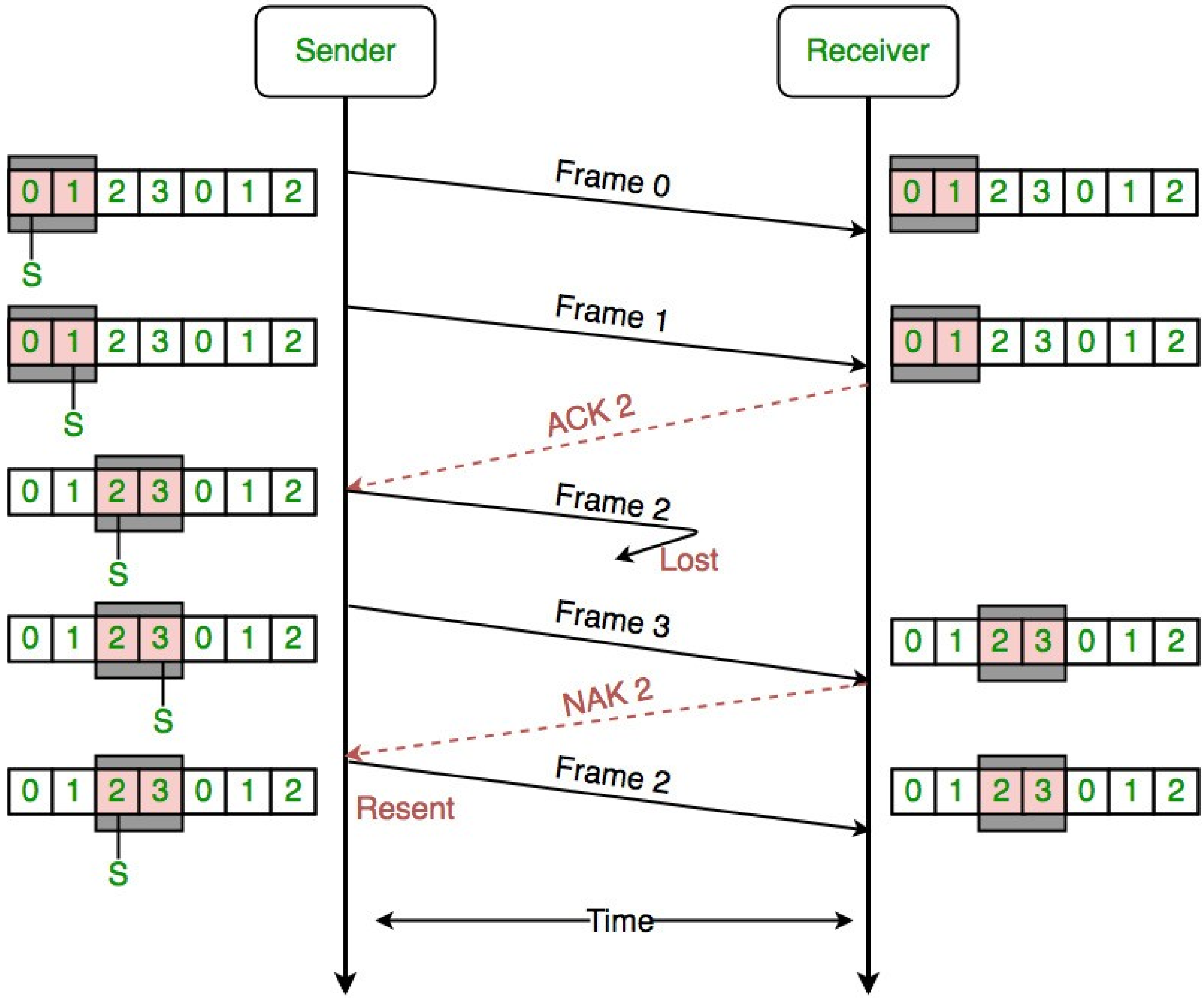


Go-Back-N ARQ –

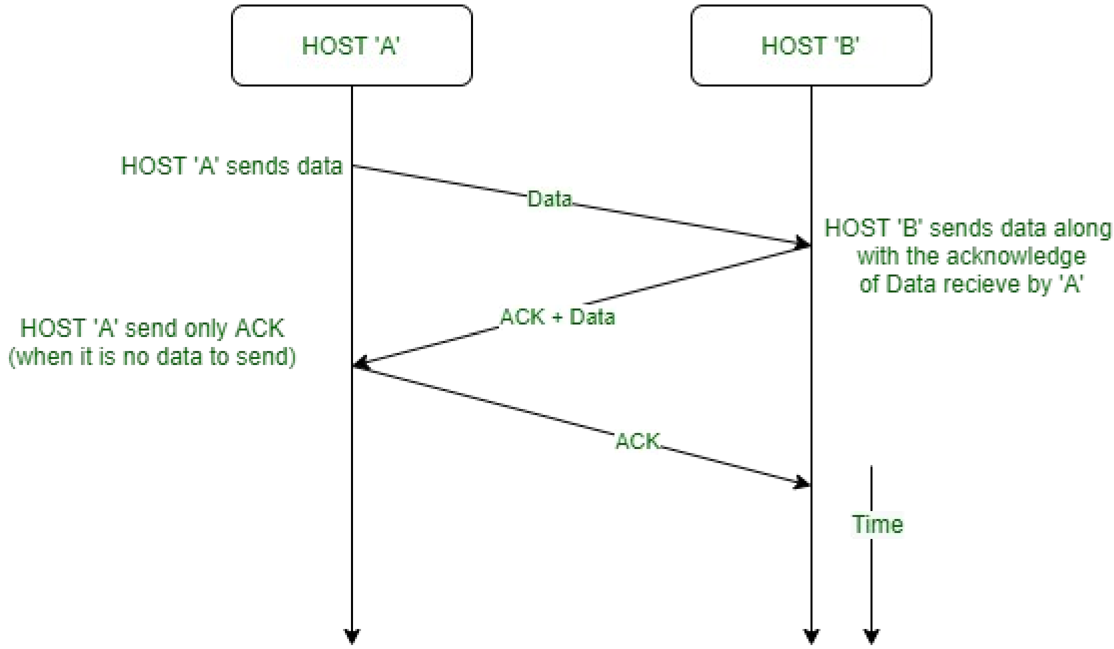


Notes : - TCP uses a sliding window for flow control.

Selective Repeat ARQ-

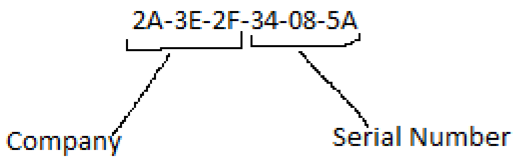


Piggybacking-



Physical Address

1. This address is available at all those devices which can be connected to network through wired or wireless media.
2. Physical address is present at NIC ROM.
3. It is also known as Hardware Address / MAC address.
4. It is attached with data frames at Data Link Layer of OSI Ref. Model. So, It is helpful in node to node delivery of data frames.
5. Ex. 2A-3D-4F-00-74-8C
6. Broadcast MAC Address = FF-FF-FF-FF-FF-FF
7. It is represented into Hexadecimal.
8. It has 12 Hexadecimal characters (48 Bits)
9. First 6 characters represents manufacturer company and last 6 characters represents serial number given by manufacturer company. So, this address is always globally unique.
10. Commands to see MAC address :
    a. C:> getmac
    b. C:> ipconfig /all
    c. ifconfig



Network Layer:

The network layer provides the functional and procedural means of transferring variable length data sequences from one node to another connected in "different networks".

Message delivery at the network layer does not give any guaranteed to be reliable network layer protocol.

Layer-management protocols that belong to the network layer are:

1. Logical Addressing – IPv4 & IPv6
2. Transition between IPv4 and IPv6
3. NAT
4. Internetworking
5. Address Mapping – ARP, RARP
6. IP Routing – Static-Manual, Dynamic – RIP, EIGRP, OSPF, BGP, IS-IS
7. Source to destination data packet delivery
8. IP Packet formation

Logical Address

2. This address is managed by Internet Protocol (IP). So, it is also known as IP address.
3. It works at Network Layer of OSI Ref. Model.
4. It is a combination of number that can be managed manually or through DHCP server. So, it is known as logical address.
5. It provides unique identity to network nodes locally or globally.
6. It is responsible for source to destination delivery of data packets.

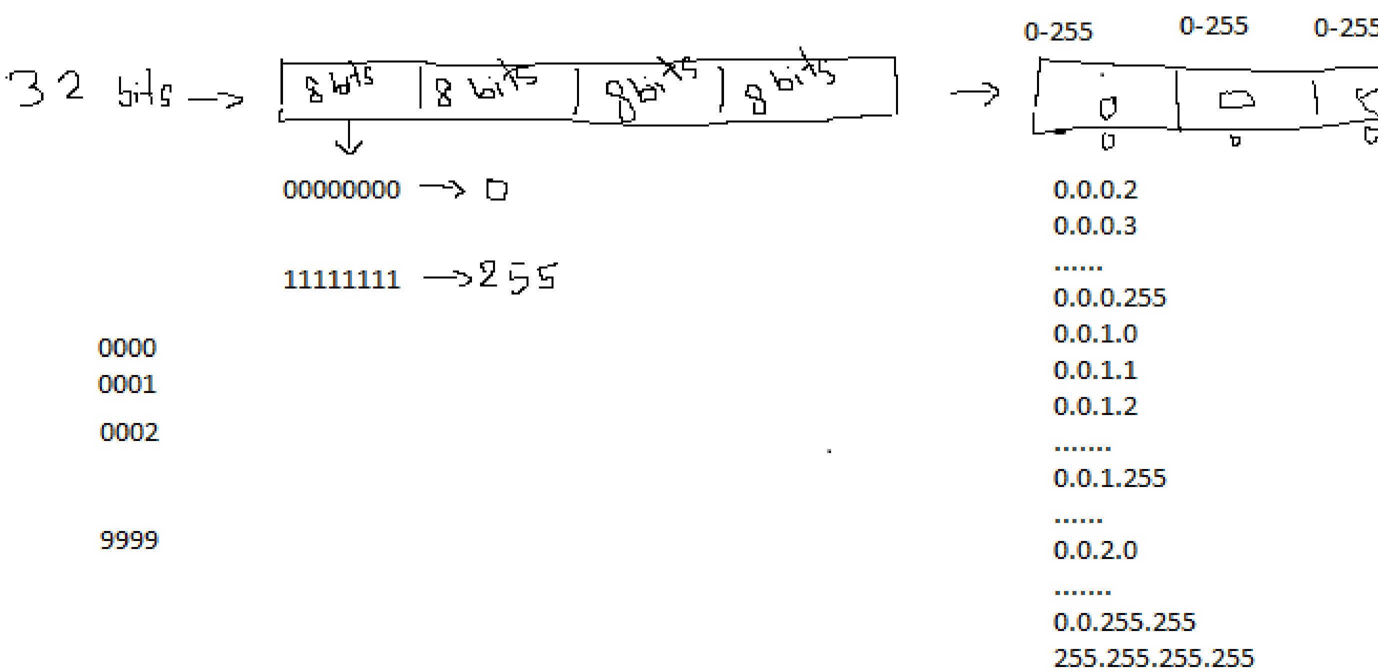
Types of IP address / Version of IP address :

1. IPv4 Address
2. IPv6 Address

IPv4 Address :

1. Developed by DARPA (Defence Advanced Research Projects Agency) in 1981.
2. Managed and distributed by IANA (Internet Assigned Number Authority).
3. Represented into dotted decimal number.
4. It has 32 bits divided into 4 groups each having 8 bits.
5. It supports approx 4.2 billion IPv4 addresses.
6. It supports unicasting, multicasting and broadcasting transmission way.
7. It is divided into 5 classes. -> A, B, C,D,E

Now, we will understand the concept of IPv4 address:



0-255			

The value of first octet is divided to form different classes.

0-127 -> Class A

128-191 -> Class B

192-223 -> Class C

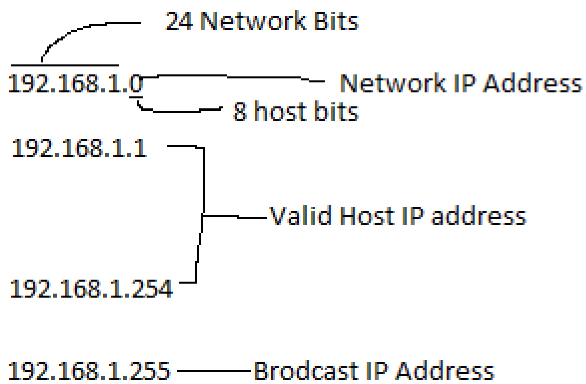
224-239 -> Class D

240 -255 -> Class E

Few important concepts before understanding these classes:

1. Network Bits – This value defines different series of IP address.
2. Host Bits – This value defines number of hosts in a network series.
3. Network IP address – The very first IP address of a network series which defines the a network.
4. Broadcast IP address – The very last IP address of a network series which is used for broadcasting in the network
5. Subnet-mask – This value defines the range of IP address in a network and defines different networks.

Example:



255.255.255.0

Class A

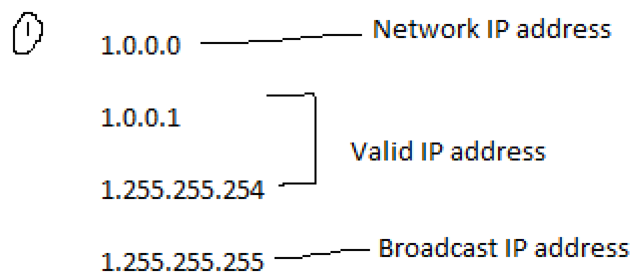
0-127	0-255	0-255	0-255

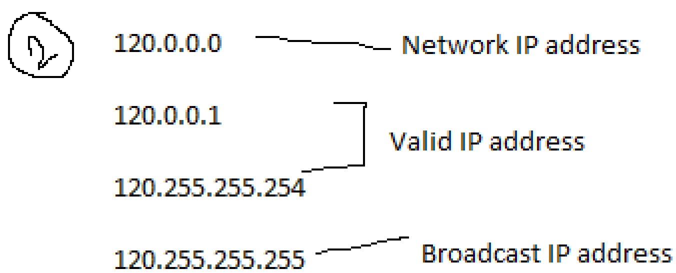
Net. Bits Host Bits Host Bits Host Bits

Important Points:

1. It has 8 bits of network and 24 bits of host.
2. Number of default networks(Blocks) = 128
3. Number of valid hosts IP address(Block Size) in each default network

= 16777216-2=16777214
4. Default subnetmask = 255.0.0.0
   Example:





Class B

128-191	0-255	0-255	0-255

Net. Bits   Net. Bits   Host Bits   Host Bits

Important Points:

1. It has 16 bits of network and 16 bits of host.
2. Number of default networks (Blocks)= 16384
3. Number of valid hosts IP address(Block Size) in each default network
   = 65536-2=65534
4. Default subnet mask = 255.255.0.0

   Example:

1

130.10.0.0 — Network IP Address

130.10.0.1
130.10.255.254
Valid Host IP address

130.10.0255.255 — Broadcast IP Address

2

130.11.0.0 — Network IP Address

130.11.0.1
130.11.255.254
Valid Host IP Address

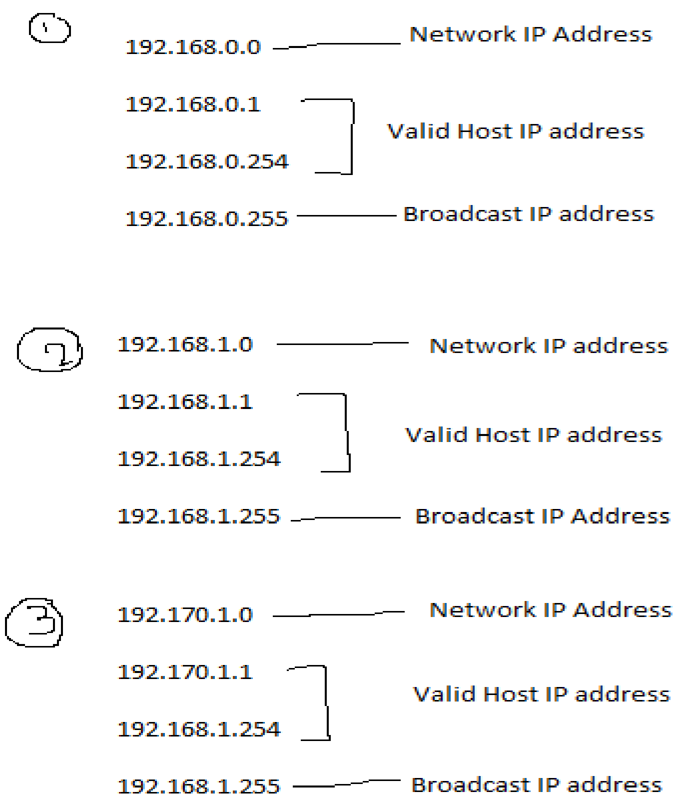
130.11.255.255 — Broadcast IP Address

Class C

192-223	0-255	0-255	0-255
Net. Bits	Net. Bits	Net. Bits	Host Bits

Important Points:

1. It has 24 bits of network and 8 bits of host.
2. Number of default networks(Blocks) = 2097152
3. Number of valid hosts IP address (Block Size)in each default network = 256-2=254
4. Default subnetmask = 255.255.255.0
   Example:



Class D

Few Points :

1. All 32 bits represents network.
2. No any host bits
3. It is used for multicasting by different services(Protocol).
   Example:
   OSPF uses 224.0.0.5 and 224.0.0.6
   RIPv2 – 224.0.0.9
   EIGRP – 224.0.0.10
   NTP – 224.0.1.1
   DHCP – 224.0.0.12
   IGMP – 224.0.0.22
   mDNS – 224.0.0.251
   Link Local Multicast IP Address – 224.0.0.252

Class E

This class is not used for any purpose.

Reserved IP Addresses:

Class A -> 0.0.0.0 -> Reserved for Default route

127.0.0.1 -> Reserved for loopback testing

Class B -> 169.254.x.y -> Reserved for APIPA, but these addresses can be used at nodes for communication.

Private IP Address

These addresses are used in local network. It does not require any reservation before use. In Class A, B and C few series have been defined as Private IP address.

Class A -> 10.0.0.0 to 10.255.255.255

Class B -> 172.16.0.0 to 172.31.255.255

Class C -> 192.168.0.0 to 192.168.255.255

Public IP Address

Those IP addresses which provides global unique identity to nodes and these must be reserved before use are known as Public IP Address. All IP addresses of Class A, B and C except reserved and private IP addresses are Public IP address.

Slash Notation of IPv4 Address:

When we use IPv4 address, subnet mask is also specified.

Slash Notation is also known as CIDR (Classless Interdomain Routing)

Ex. -> 10.0.0.1 -> IPv4 address

255.0.0.0 -> subnet mask

The above address and subnet mask can be used with slash.

Ex. -> 10.0.0.1/8

172.16.0.10/16

192.168.0.1/24

To identify the class of IPv4 if it is represented into Binary number system:

1. Class A

   Range -> 0-127

   In Binary -> 00000000 - 01111111

   Conclusion : If first one bit is 0 IP will belong to Class A.

2. Class B

   Range -> 128 - 191

   In Binary -> 10000000 - 10111111

   Conclusion : If first two bits are 10 IP will belong to Class B.

3. Class C

   Range -> 192-223

   In Binary -> 11000000 - 11011111

   Conclusion : If first 3 bits are 110 IP will belong to Class C.

4. Class D

   Range -> 224-239

   In Binary -> 11100000 - 11101111

   Conclusion : If first 4 bits are 1110 IP will belong to Class D.

Classfull IPv4 address:

All default, IPv4 address with default subnetmask represents Classfull IPv4 address.

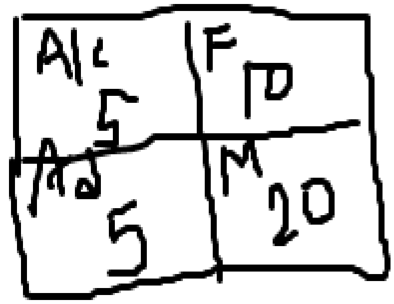
Classless IPv4 address:

In Classless IPv4 address, Default series of IPv4 address is divided into small subnets or large subnets by changing the value of default subnetmask. Subnetmask defines the network and host bits in IP address.

Subnetting :

It is process by which a default series of IPv4 address is divided into small and equal subnets.

There are 4 departments .
All these departments should be in diff network.



Total IP used - 1024
Nodes - 40

Heavy loss of IP add

A/c - 192.168.0.0 - 256
Faculty - 192.168.1.0 - 256
Admin - 192.168.2.0 - 256
Marketing - 192.168.3.0 - 256

Now we will use subnetting to break a single series of IP to form multiple subnets.

Max Requirement - 20+2=22

Block Size = 32

Host Bits = 5
Total Bits in IPv4 = 32
Network Bits = 27
11111111.11111111.11111111.11100000
255.255.255. 224

1
2
4
8
16
Host Bits =5
32 Block Size
64
128
256
512
1024
.....

Now, We will take ->
192.168.0.0
255.255.255.0
192.168.0.0 - 192.168.0.255
Total IP add - 256
We can make multiple subnets of 32 IP add. - 8 subnets

Default Net. Bits in Class C = 24
Net. Bits in this subnet = 27
Extra Net. Bits = 3
So, No. of subnets = 2^ Extra Net. Bits
= 2^3 = 8

Subnetmask = 11111111.11111111.111111111.11100000

32

1. Marketing
Req PC - 20
192.168.0.0 — Network IP Add
192.168.0.1
.
.
192.168.0.30

Valid Host IP Add

192.168.0.31 — Broad Cast IP Add

Subnetmask =
255.255.255.224

2. Faculty - Req. PC = 10
192.168.0.32
192.168.0.33
.
.
192.168.0.62
192.168.0.63

Subnetmask =
255.255.255.224

0 0 - 31
+32
32 32-63
+32
64 64 - 95
+32
96 96 - 127
+32
128

1
2
4
8
16
32
64
128
256
512
1024
2048
4096
8192
......

VLSM (Variable Length Subnet Mask)

It is process by which a default series of IPv4 address is divided into small and unequal subnets.

Req. - 100, 50, 20, 10

Class C - 256 ip add - > 192.168.0.0   255.255.255.0

1 st Network -
Max . Req - 100+2=102
Block Size = 128
Host Bits - 7
Net Bits - 25
Subnetmask - 11111111.11111111.11111111.10000000 — 128
255.255.255.128

192.168.0.0
192.168.0.1

192.168.0.126
192.168.0.127

0   0-127
128
128
64   128 — 191
192
192   192 — 223
32
224   224 — 239
+ 16
240

2nd Network
Max. Req -50+2=52
Block Size - 64
Host Bits - 6
Net Bits = 26
Subnetmask = 11111111.11111111.11111111.11000000 — 64
255.255.255.192

192.168.0.128
192.168.0.129

192.168.0.190
192.168.0.191

3rd Network -
Max . Re. - 20+2=22
Block Size - 32
Host BIts - 5
NEt BIts- 27
11111111.11111111.11111111.11100000 — 32
255.255.255.224
192.168.0.192 - 192.168.0.223

4th NEt.
Max. Req = 10+2=12
Block Size,=16, Net. Bits = 28, Host Bits= 4
Subnetmask = 11111111.11111111.11111111.11110000 — 16
255.255.255.240

192.168.0.224 - 192.168.0.239

Hw- 50, 20, 10, 5
Class C- 192.168.0.0

Supper-netting:

Default two or more series of Class C are combined to form a large network.

Supernetting -

Req. - 500+2=502 Block Size - 512 2
Host Bits - 9
Net. Bits - 23
11111111.11111111.11111110.00000000
255.255.254.0

9
+2 2 n-1
2

1000
Block Size = 1024
Host Bits = 10
Net Bits = 22
255.255.252.0

Class C -
192.168.0.0 Network IP Address
192.168.0.1

192.168.0.255
192.168.1.0 Valid Host IP Address
192.168.1.1

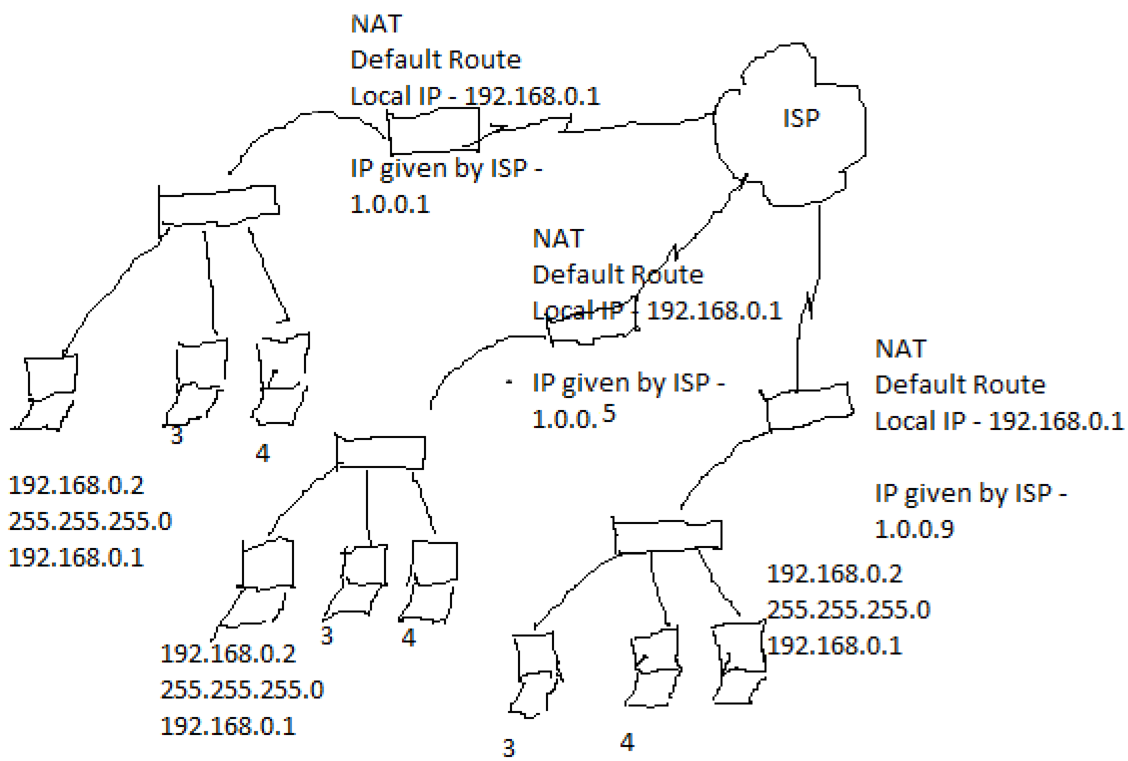
192.168.1.254
192.168.1.255 Broadcast IP Address

Class C -
192.168.0.0 Net. IP Add
192.168.0.1
Valid Host IP Addre
192.168.3.254
192.168.3.255 Broadcast IP A

Home Work -
Req. 1000 PC
IP Class C

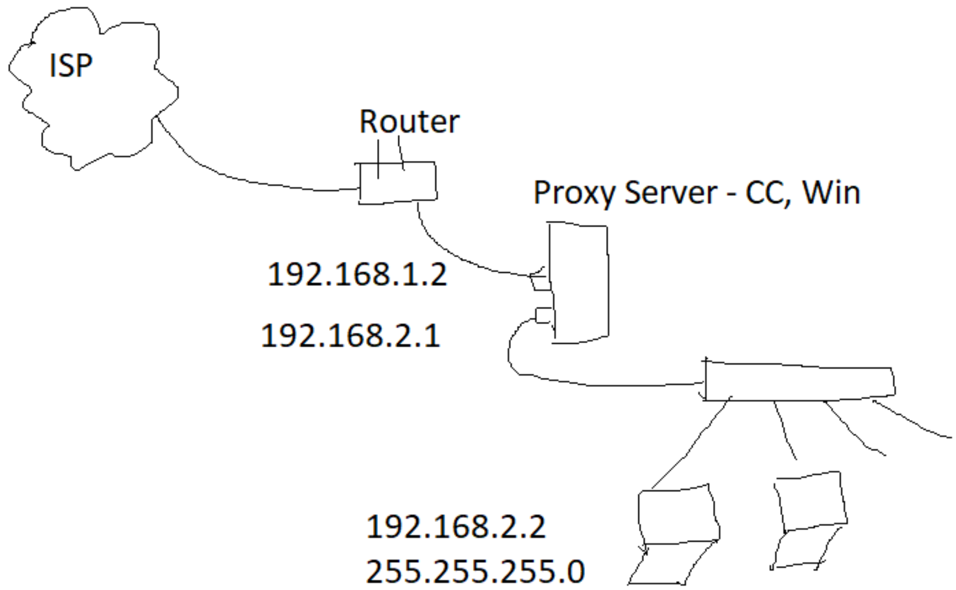
NAT (Network Address Translation):

1. It is Protocol or service that is used to convert inside local IP address into outside global IP address.
2. It is mostly used by ISP or used at router to provide internet service at private IP address through IP provided by ISP.
3. It provides security in the network.
4. It conserves IP addresses.



Proxy Server

1. It is used for internet service.
2. It provides security by hiding internal network.
3. It provides different security features like – website restriction, data limit, log generation, etc.
4. It provides fault tolerance.



IPv6 Address:

1. IPv6 was introduced in Dec, 1998.
2. Developed by IETF.
3. It was developed due to exhaustion of IPv4 address.
4. Launched in 6 June, 2012
5. It has 128 bits divided into 8 groups each having 16 bits.
6. Represented into Hexadecimal Number System.
7. Each group is separated by colon(:).
8. It supports approx 3.4*10^38 IPv6 addresses.
9. These addresses supports unicasting, multicasting and anycasting.
10. There is no any class like IPv4
11. There is no any network IP address and broadcast IP address.
12. By default its first 64 bits represents Network Bits and last 64 bits represents host bits.
13. There is no any subnetmask.
14. Network Bits are represented as Subnet prefix length.

2000:0000:0000:001a:002b:001d:002c:0012

64

Example:

Net.Bits	Net.Bits	Net.Bits	Net.Bits	Host Bit	Host Bit	Host Bit	Host Bit

16 Bits	16 Bits	16 Bits	16 Bits	16 Bits	16 Bits	16 Bits	16 Bits

These 16 bits are represented into hexadecimal.

0000	0000	0000	0000	0000	0000	0000	0000

This is the very first IPv6 address.

FFFF	FFFF	FFFF	FFFF	FFFF	FFFF	FFFF	FFFF

This is the very last IPv6 address
Now, we will understand the flow of this addess.

0000
0001
0002
0003
....
000F
0010
0011
....
001F
0020
....
002F
....
FFFF

In this way, a single group can generate 65,536 different number.

Simply, Total IPv6 address = 65,536^8

Few important points about the use of IPv6 address:

1. we can use abbreviation to reduce the length of IPv6 address.

   Ex.1 - 2000:0000:0000:0001:0000:0000:0000:001a/64

   2000:0:0:1::1a/64

   Ex.2 - 2000:0000:0000:0001:0000:0000:000a:001a/64

   2000::1:0:0:a:1a/64

2. The very first IPv6 address is known as unknown address.

   ::/128

3. The very first IPv6 address ::/0 is used for default route.
4. ::1 -> It is known as loopback address.
5. The address range that start with FE80:: is known as Link Local IP address. This

   address is assigned to each interface automatically.

6. The address that start with FF0 is known as multicast IPv6 address:

   FF05 - OSPFv3

   FF06 - OSPFv3

   FF09 - RIPng

   FF0A - EIGRP

7. EUI(Extended Unique Identifier) Format of IPv6:

   In this format, last 64 Host bits can be form automatically by node with the help of MAC address assigned at interface.

Example:

Interface MAC address: 2A-3B-2C-3D-4F-5A

2000	0000	0000	0001	2A3B	2C_ _	_ _3D	4F5A

64 Network Bits ---------------------------------| 64 Host Bits ----------------------------------|

In last 64 bits MAC address is used. But, it gives only 48 bits for rest 16 bits FFFE is used. It is done automatically.

Finally, the address will be

2000	0000	0000	0001	2A3B	2CFF	FE 3D	4F5G

Example of different network :

1. 2000:a:b:1::/64

2000	000a	000b	0001	0000	0000	0000	0000

This is the very first IPv6 address of this network.

2000	000a	000b	0001	ffff	ffff	ffff	ffff

This is the very last IPv6 address of this network.

2. 2000:a:b:2::/64

2000	000a	000b	0002	0000	0000	0000	0000

This is the very first IPv6 address of this network.

2000	000a	000b	0002	ffff	ffff	ffff	ffff

This is the very last IPv6 address of this network.

IP Packet:

TRANSITION FROM IPv4 TO IPv6

Because of the huge number of systems on the Internet, the transition from IPv4 to IPv6 cannot happen suddenly. It takes a considerable amount of time before every system in the Internet can move from IPv4 to IPv6. The transition must be smooth to prevent any problems between IPv4 and IPv6 systems. Three strategies have been devised by the !ElF to help the transition.

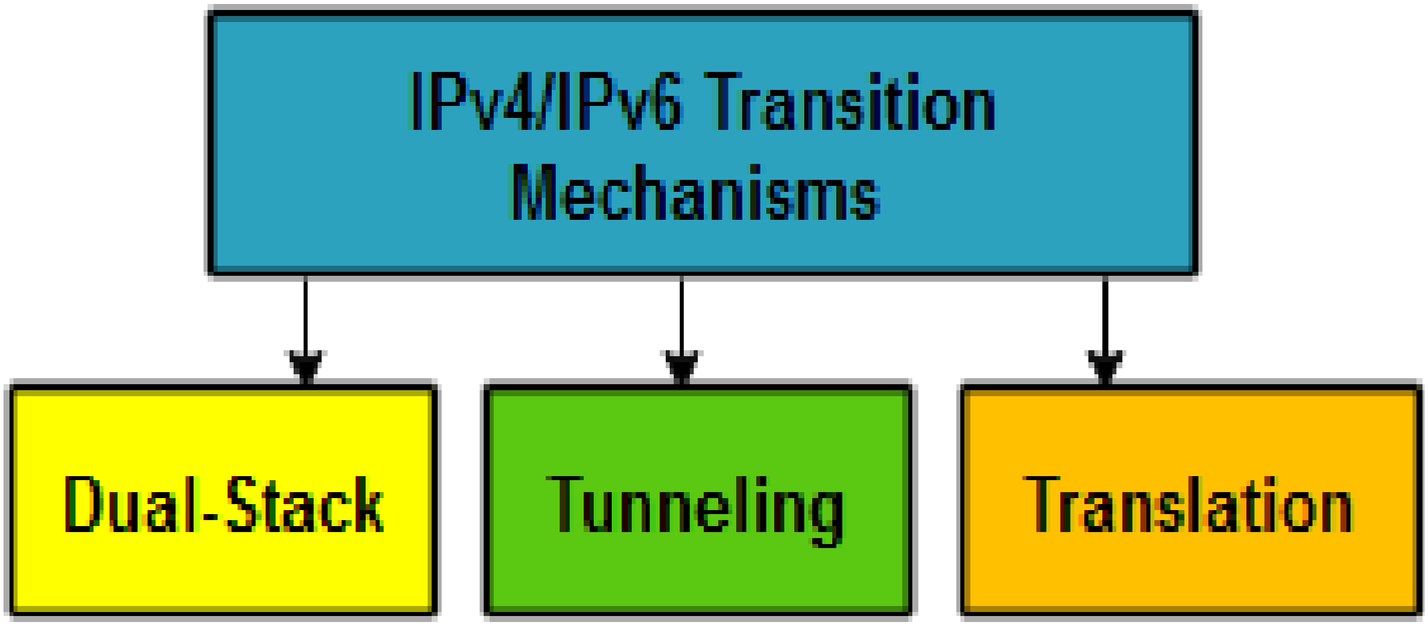


Fig. 1 IPv4/IPv6 transition mechanisms classification

Dual Stack:-

In dual stack, a node should use both IPv4 and IPv6 addresses for communication with any network based on IPv4 or IPv6 addresse.

Tunneling –

Tunneling is a strategy used when two computers using IPv6 want to communicate with each other and the packet must pass through a region that uses IPv4. To pass through this region, the packet must have an IPv4 address. So the IPv6 packet is encapsulated in an IPv4 packet when it enters the region, and it leaves its capsule when it exits the region.

Header Translation:-

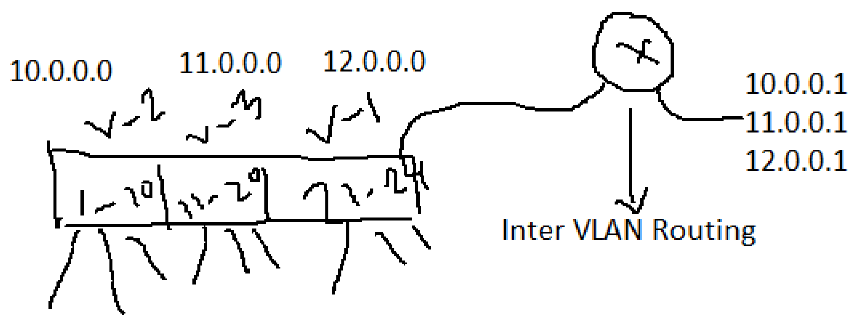
Header translation is necessary when the majority of the Internet has moved to IPv6 but some systems still use IPv4. The sender wants to use IPv6, but the receiver does not understand IPv6. Tunneling does not work in this situation because the packet must be in the IPv4 format to be understood by the receiver. In this case, the header format must be totally changed through header translation.

Address Mapping –

Address mapping is a technique by which IP add and MAC address are mapped into a table. With this table, a node can communicate in a LAN or WAN. Protocols used for address Mapping – ARP, RARP

VLAN –

It is process by which switch ports are divided into multiple groups to from different LAN at switch. Different VLANs are identified by VLAN ID (1-4094). Different VLANs can communicate to each other if they are based on different subnet of IP address. This is known as VLAN routing. It is done with the help of L3 device.



What is IP routing?

It is process by which best route is defined into routing table. With this route data is transferred between source to destination network.

Types of IP routing:

1. **Static Rouing – In this routing, routes are defined manually.**
   #ip route <Des. Net. IP> <Sub. Mask> <Next hop router add>

2. **Static Default – In this routing, a single route is defined to communicate with all destination networks.**
   #ip route 0.0.0.0 0.0.0.0 <next hop router address / ISP router>
3. **Dynamic Routing – In this routing, best routes are defined by routing Protocols. Ex – RIP, RIPv2, OSPF, EIGRP, IGRP, BGP, IS-IS.**
   Types of Dynamic Routing:-

   Routing Based on Broadcast – A routing process which is done by a router / server / L3 switch that is base on broadcasting. It uses 255.255.255.255 broadcast address to send routing table update. It is also known as "Routing by Rumor". It is mostly done at fixed interval of time. It is suitable for small network.
   Ex – RIP, BGP

   Routing Based on Multicast:-
   A routing process which is by a router/ server/ L3 switch that is based on multicasting. Different routing protocols use different multicast IP address. It is also known as Routing by Intelligence. It sends triggered update means when ever any change occur in the network. It is suitable for a large network.
   Ex-
   OSPF – IPv4 based – 224.0.0.5, 224.0.0.6
   OSPF – Ipv6 Based – FF05:: , FF06::

IPX (Internetwork Packet Exchange)

IPX is a networking protocol that conducts the activities and affairs of the end-to-end process of timely, managed and secured data. Originally used by the Novell NetWare operating system and it was later adopted by Windows. As they replaced NetWare LANS they became widely used on

networks deploying Microsoft Windows LANs. IPX/SPX or Internetwork Packet Exchange/Sequenced Packet Exchange was developed by Novell to be a replacement to the TCP/IP Protocol Suite. This was introduced in Novell's networking software called Netware in the early 1980s. IPX introduced in the 1980s remained fairly popular till the 1990s. After which the TCP/IP protocol has largely replaced it.

Working of IPX

IPX is the network layer and SPX is the transport layer of the IPX/SPX network protocol. IPX and IP protocol have similar functions and this defines how data is sent and received between devices. The transport layer protocol or SPX protocol is used to establish and maintain a connection between devices. Together, they can be used to transfer data and create a network connection between systems.

IPX does not require a consistent connection to be maintained while packets are being sent from one system to another, this is what is called being connectionless. It can resume the transfer from the point where it was interrupted due to bad connection or power loss.

Applications

IPX provides peer-to-peer support connectivity. Like IP, IPX also contains end-user data and is connectionless, just like network addresses. Novell's original NetWare client was written for DOS. In the 1990s, video games like Quake, Descent, and WarCraft 2 were supported with IPX for network gaming. Kali was the name of a service used as an emulator to let gamers play online

Advantages

- IPX/SPX was primarily designed for local area networks (LANs) and is very efficient when used for this only.
- IPX has a larger address space: 48 bits instead of 32 bits in IPv4.
- IPX addresses incorporate the local MAC address:compared to "address assignment" like with IPv4.
- No BootP or DHCP in IPX. (DHCP was invented from BootP was so that IPv4 could allow "plug-and-go" network addressing like what IPX did. It was later added in IPv6.)

Disadvantages

- Nowadays IPX is falling out of trend. TCP/IP is mostly used because of its superior performance over wide area networks and the Internet and its a more mature protocol created with the same purpose in mind. The real advantage of TCP/IP is interoperability and vendor-independent open standards.
- With IPX applications and the use of the internet, the costs are higher if you are implementing VPNs.

- Encapsulating and encrypting of IPX frames in an IP packet requires expensive hardware than performing a straight IPSec VPN.

Apple Talk

AppleTalk is a proprietary networking protocol used with Apple Macintosh computers and networking devices to communicate with each other that was first introduced in 1984. In 2009, with the release of macOS X v10.6, this networking protocol was replaced by TCP/IP.

AppleTalk is a workgroup-level networking technology that supports up to 254 network nodes per physical network.

Transport Layer:

The transport layer builds on the network layer to provide data transport from a process on a source machine to a process on a destination machine. It is hosted using single or multiple networks, and also maintains the quality of service functions.

It determines how much data should be sent where and at what rate. This layer builds on the message which are received from the application layer. It helps ensure that data units are delivered error-free and in sequence.

Transport layer helps you to control the reliability of a link through flow control, error control, and segmentation or de-segmentation.

The transport layer also offers an acknowledgment of the successful data transmission and sends the next data in case no errors occurred. TCP is the best-known example of the transport layer.

Important functions of Transport Layers:

- The transport layer is responsible for process-to-process delivery of the entire message. A process is an application program running on a host.
- It divides the message received from the session layer into segments and numbers them to make a sequence.
- Transport layer makes sure that the message is delivered to the correct process on the destination machine.
- It also makes sure that the entire message arrives without any error else it should be retransmitted.

- Service-point addressing / Port Addressing
- Segmentation and reassembly
- Connection control
- Flow control
- Error control

UDP (User Datagram Protocol)

It does not support acknowledgement. So, it is unreliable.

TCP (Transmission Control Protocol)

SCTP

SCTP stands for **Stream Control Transmission Protocol**.
It is a connection- oriented protocol in computer networks which provides a full-duplex association i.e., transmitting multiple streams of data between two end points at the same time that have established a connection in network. It is sometimes referred to as next generation TCP or TCPng, SCTP makes it easier to support telephonic conversation on Internet. A telephonic conversation requires transmitting of voice along with other data at the same time on both ends, SCTP protocol makes it easier to establish reliable connection.

SCTP is also intended to make it easier to establish connection over wireless network and managing transmission of multimedia data. SCTP is a standard protocol (RFC 2960) and is developed by Internet Engineering Task Force (IETF).

CONGESTION

An important issue in a packet-switched network is congestion. Congestion in a network may occur if the load on the network-the number of packets sent to the network-is greater than the capacity of the network-the number of packets a network can handle. Congestion control refers to the mechanisms and techniques to control the congestion and keep the load below the capacity.

A router, for example, has an input queue and an output queue for each interface. When a packet arrives at the incoming interface, it undergoes three steps before departing.

CONGESTION CONTROL

Congestion control refers to techniques and mechanisms that can either prevent congestion, before it happens, or remove congestion, after it has happened.

Congestion Control categories-

Open Loop (Prevention from congestion)

a. Retransmission policy- If the sender feels that a sent packet is lost or corrupted, the packet needs to be retransmitted.
b. Window policy - The Selective Repeat window is better than the Go-Back-N window for congestion control. In the Go-Back-N window, when the timer for a packet times out, several packets may be resent, although some may have arrived safe and sound at the receiver. This duplication may make the congestion worse. The Selective Repeat window, on the other hand, tries to send the specific packets that have been lost or corrupted
c. Acknowledgment policy- Acknowledgment is sent by the receiver.
d. Discarding policy – Discard received packets to prevent duplication of data and to reduce load.
e. Admission policy - An admission policy, which is a quality-of-service mechanism, can also prevent congestion in virtual-circuit networks. Switches in a flow first check the resource requirement of a flow before admitting it to the network. A router can deny establishing a virtualcircuit connection if there is congestion in the network or if there is a possibility of future congestion.

Closed Loop (Removal of congestion)

a. Back pressure - The technique of backpressure refers to a congestion control mechanism in which a congested node stops receiving data from the immediate upstream node or nodes. This may cause the upstream node or nodes to become congested, and they, in turn, reject data from their upstream nodes or nodes. And so on. Backpressure is a node-to-node congestion control that starts with a node and propagates, in the opposite direction of data flow, to the source. The backpressure technique can be applied only to virtual circuit networks, in which each node knows the upstream node from which a flow of data is corning.
b. Choke packet - A choke packet is a packet sent by a node to the source to inform it of congestion.
c. Implicit signaling - In implicit signaling, there is no communication between the congested node or nodes and the source.
d. Explicit signaling - The node that experiences congestion can explicitly send a signal to the source or destination.

Flow Control-

Characteristics of data flow-

Reliability - Lack of reliability means losing a packet or acknowledgment, which entails retransmission.

Delay – Network should have less delay in data transmission.

Jitter - Jitter is the variation in delay for packets belonging to the same flow.

Bandwidth – Discussed earlier.

Techniques to improve data flow :

Scheduling

a. FIFO Queuing - In first-in, first-out (FIFO) queuing, packets wait in a buffer (queue) until the node (router or switch) is ready to process them. Ifthe average arrival rate is higher than the average processing rate, the queue will fill up and new packets will be discarded. A FIFO queue is familiar to those who have had to wait for a bus at a bus stop.
b. Priority Queuing - In priority queuing, packets are first assigned to a priority class. Each priority class has its own queue. The packets in the highest-priority queue are processed first. Packets in the lowest-priority queue are processed last. Note that the system does not stop serving a queue until it is empty.
c. Weighted Fair Queuing - In this technique, the packets are still assigned to different classes and admitted to different queues. The queues, however, are weighted based on the priority of the queues; higher priority means a higher weight. The system processes packets in each queue in a round-robin fashion with the number of packets selected from each queue based on the corresponding weight. For example, if the weights are 3, 2, and 1, three packets are processed from the first queue, two from the second queue, and one from the third queue. If the system does not impose priority on the classes, all weights can be equal In this way, we have fair queuing with priority. Figure 24.18 shows the technique with three classes

Session Layer

Session Layer controls the dialogues between computers. It helps you to establish starting and terminating the connections between the local and remote application.

This layer request for a logical connection which should be established on end user's requirement. This layer handles all the important log-on or password validation.

Session layer offers services like dialog discipline, which can be duplex or half-duplex. It is mostly implemented in application environments that use remote procedure calls.

Important function of Session Layer:

- It establishes, maintains, and ends a session.
- Session layer enables two systems to enter into a dialog
- It also allows a process to add a checkpoint to steam of data.
- Dialog control
- Synchronization

Presentation Layer

Presentation layer allows you to define the form in which the data is to exchange between the two communicating entities. It also helps you to handles data compression and data encryption.

This layer transforms data into the form which is accepted by the application. It also formats and encrypts data which should be sent across all the networks. This layer is also known as a **syntax layer**.

The function of Presentation Layers:

- Character code translation from ASCII to EBCDIC.
- Data compression: Allows to reduce the number of bits that needs to be transmitted on the network.
- Data encryption: Helps you to encrypt data for security purposes — for example, password encryption.
- It provides a user interface and support for services like email and file transfer.
- Encryption / Decryption
- Compression / Decompression

Application Layer

- Application Layer provides a facility by which users can forward several emails and it also provides a storage facility.
- This layer allows users to access, retrieve and manage files in a remote computer.
- It allows users to log on as a remote host.

- This layer provides access to global information about various services.
- This layer provides services which include: e-mail, transferring files, distributing results to the user, directory services, network resources and so on.
- It provides protocols that allow software to send and receive information and present meaningful data to users.
- It handles issues such as network transparency, resource allocation and so on.
- This layer serves as a window for users and application processes to access network services.
- Application Layer is basically not a function, but it performs application layer functions.
- The application layer is actually an abstraction layer that specifies the shared protocols and interface methods used by hosts in a communication network.
- Application Layer helps us to identify communication partners, and synchronizing communication.
  - This layer allows users to interact with other software applications.
  - In this layer, data is in visual form, which makes users truly understand data rather than remembering or visualize the data in the binary format (0's or 1's).
  - This application layer basically interacts with Operating System (OS) and thus further preserves the data in a suitable manner.
  - This layer also receives and preserves data from it's previous layer, which is Presentation Layer (which carries in itself the syntax and semantics of the information transmitted).
  - The protocols which are used in this application layer depend upon what information users wish to send or receive.
  - This application layer, in general, performs host initialization followed by remote login to hosts.

DNS(Domain Name System)

Flat Name Space

In a flat name space, a name is assigned to an address. A name in this space is a sequence of characters without structure. The names mayor may not have a common section; if they do, it has no meaning. The main disadvantage of a fiat name space is that it cannot be used in a large system such as the Internet because it must be centrally controlled to avoid ambiguity and duplication. – (**NetBIOS**)

Hierarchical Name Space

In a hierarchical name space, each name is made of several parts. The first part can define the nature ofthe organization, the second part can define the name of an organization, the third part can define departments in the organization, and so on. – www.google.com → Host – www, Domain – google, Zone – com (FQDN – Fully Qualified Domain Name) → (**DNS, DDNS**)

Resolver

DNS is designed as a client/server application. A host that needs to map an address to a name or a name to an address calls a DNS client called a resolver. The resolver accesses the closest DNS server with a mapping request. If the server has the information, it satisfies the resolver; otherwise, it either refers the resolver to other servers or asks other servers to provide the information.

Mapping Names to Addresses

Most of the time, the resolver gives a domain name to the server and asks for the corresponding address. In this case, the server checks the generic domains or the country domains to find the mapping. If the domain name is from the generic domains section, the resolver receives a domain name such as "chal.atc.jhda.edu.". The query is sent by the resolver to the local DNS server for resolution. If the local server cannot resolve the query, it either refers the resolver to other servers or asks other servers directly. If the domain name is from the country domains section, the resolver receives a domain name such as "ch.jhda.cu.ca.us.". The procedure is the same. – **Host Record(A / AAA)** – Used for name to address mapping.

Mapping Addresses to Names

A client can send an IP address to a server to be mapped to a domain name. As mentioned before, this is called a PTR query. To answer queries of this kind, DNS uses the inverse domain. However, in the request, the IP address is reversed and the two labels in-addr and arpa are appended to create a domain acceptable by the inverse domain section. – **PTR Record** – used for IP add to name mapping

Recursive Resolution

The client (resolver) can ask for a recursive answer from a name server. This means that the resolver expects the server to supply the final answer. If the server is the authority for the domain name, it checks its database and responds. Ifthe server is not the authority, it sends the request to another server (the parent usually) and waits for the response. If the parent is the authority, it responds; otherwise, it sends the query to yet another server. When the query is

finally resolved, the response travels back until it finally reaches the requesting client. This is called recursive resolution.

Iterative Resolution

If the client does not ask for a recursive answer, the mapping can be done iteratively. If the server is an authority for the name, it sends the answer. If it is not, it returns (to the client) the IP address of the server that it thinks can resolve the query. The client is responsible for repeating the query to this second server. If the newly addressed server can resolve the problem, it answers the query with the IP address; otherwise, it returns the IP address of a new server to the client. Now the client must repeat the query to the third server. This process is called iterative resolution because the client repeats the same query to multiple servers.

Caching

Each time a server receives a query for a name that is not in its domain, it needs to search its database for a server IP address. Reduction of this search time would increase efficiency. DNS handles this with a mechanism called caching. When a server asks for a mapping from another server and receives the response, it stores this information in its cache memory before sending it to the client. If the same or another client asks for the same mapping, it can check its cache memory and solve the problem. However, to inform the client that the response is coming from the cache memory and not from an authoritative source, the server marks the response as un-authoritative. Caching speeds up resolution, but it can also be problematic. If a server caches a mapping for a long time, it may send an outdated mapping to the client. To counter this, two techniques are used. First, the authoritative server always adds information to the mapping called time-to-live (TTL). It defines the time in seconds that the receiving server can cache the information. After that time, the mapping is invalid and any query must be sent again to the authoritative server. Second, DNS requires that each server keep a TTL counter for each mapping it caches. The cache memory must be searched periodically, and those mappings with an expired TTL must be purged.

DYNAMIC DOMAIN NAME SYSTEM (DDNS)

When the DNS was designed, no one predicted that there would be so many address changes. In DNS, when there is a change, such as adding a new host, removing a host, or changing an IP address, the change must be made to the DNS master file. These types of changes involve a lot of manual updating. The size of today's Internet does not allow for this kind of manual operation. The DNS master file must be updated dynamically. The Dynamic Domain Name System (DDNS) therefore was devised to respond to this need. In DDNS, when a binding between a name and an address is determined, the information is sent, usually by DHCP (see Chapter 21) to a primary

DNS server. The primary server updates the zone. The secondary servers are notified either actively or passively. In active notification, the primary server sends a message to the secondary servers about the change in the zone, whereas in passive notification, the secondary servers periodically check for any changes. In either case, after being notified about the change, the secondary requests information about the entire zone (zone transfer). To provide security and prevent unauthorized changes in the DNS records, DDNS can use an authentication mechanism.

TELNET

TELNET is an abbreviation for Terminal Network. It is the standard TCP/IP protocol for virtual terminal service as proposed by the International Organization for Standards (ISO). TELNET enables the establishment of a connection to a remote system in such a way that the local terminal appears to be a terminal at the remote system. TELNET is a general-purpose client/server application program.

SSh (Secure Shell)

MIME (Multipurpose Internet Mail Extensions)

Electronic mail has a simple structure. Its simplicity, however, comes at a price. It can send messages only in NVT 7-bit ASCII format. In other words, it has some limitations. For example, it cannot be used for languages that are not supported by 7-bit ASCII characters (such as French, German, Hebrew, Russian, Chinese, and Japanese). Also, it cannot be used to send binary files or video or audio data. Multipurpose Internet Mail Extensions (MIME) is a supplementary protocol that allows non-ASCII data to be sent through e-mail. MIME transforms non-ASCII data at the sender site to Non- ASCII data and delivers them to the client to be sent through the Internet. The message at the receiving side is transformed back to the original data. We can think of MIME as a set of software functions that transforms non-ASCII.

SMTP (Simple Mail Transfer Protocol)

POP3 (Post Office Protocol version 3)

POP3 is simple and limited in functionality. The client POP3 software is installed on the recipient computer; the server POP3 software is installed on the mail server. Mail access starts with the client when the user needs to download e-mail from the mailbox on the mail server. The client opens a connection to the server on TCP port 110. It then sends its user name and password to

access the mailbox. The user can then list and retrieve the mail messages, one by one. Figure 26.20 shows an example of downloading using POP3. POP3 has two modes: the delete mode and the keep mode. In the delete mode, the mail is deleted from the mailbox after each retrieval. In the keep mode, the mail remains in the mailbox after retrieval. The delete mode is normally used when the user is working at her permanent computer and can save and organize the received mail after reading or replying. The keep mode is normally used when the user accesses her mail away from her primary computer (e.g., a laptop). The mail is read but kept in the system for later retrieval and organizing.

IMAP4 (Internet Mail Access Protocol version 4)

Another mail access protocol is Internet Mail Access Protocol, version 4 (IMAP4). IMAP4 is similar to POP3, but it has more features; IMAP4 is more powerful and more complex.

Important Features of IMAP4

- A user can check the e-mail header prior to downloading.
- A user can search the contents of the e-mail for a specific string of characters prior to downloading.
- A user can partially download e-mail. This is especially useful if bandwidth is limited and the e-mail contains multimedia with high bandwidth requirements.
- A user can create, delete, or rename mailboxes on the mail server.
- A user can create a hierarchy of mailboxes in a folder for e-mail storage

File Transfer Protocol (FTP)

File Transfer Protocol (FTP) is the standard mechanism provided by TCP/IP for copying a file from one host to another. Although transferring files from one system to another seems simple and straightforward, some problems must be dealt with first. For example, two systems may use different file name conventions. Two systems may have different ways to represent text and data. Two systems may have different directory structures. All these problems have been solved by FTP in a very simple and elegant approach. FTP differs from other client/server applications in that it establishes two connections between the hosts. One connection is used for data transfer, the other for control information (commands and responses). Separation of commands and data transfer makes FTP more efficient. The control connection uses very simple rules of communication. Wc need to transfer only a line of command or a line of response at a time. The data connection, on the other hand, needs more complex rules due to the variety of data types transferred. However, the difference in complexity is at the FTP level, not TCP. For TCP, both connections are treated the same. FTP uses two well-known TCP ports: Port 21 is used for the control connection, and port 20 is used for the data connection.

HTTP

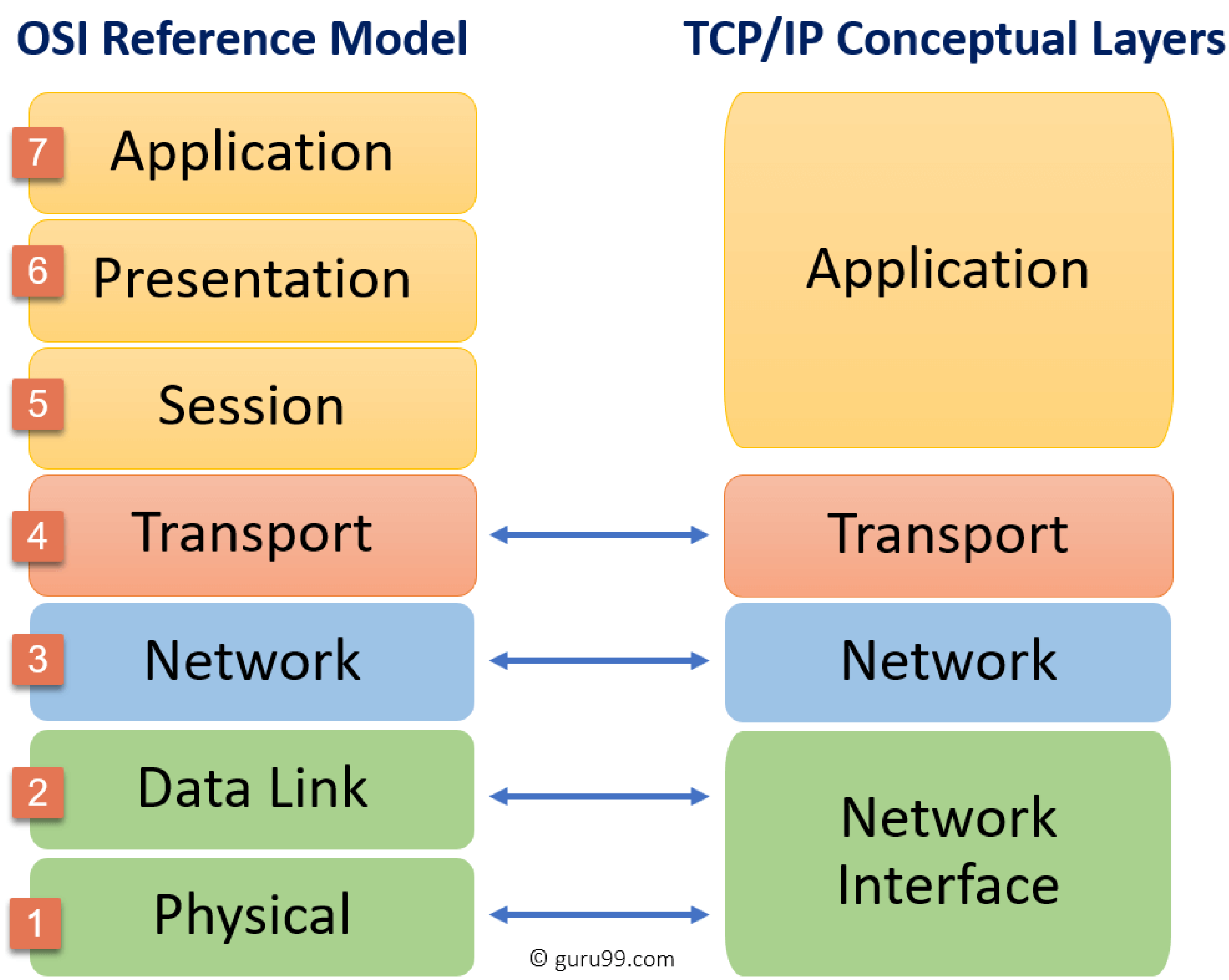
HTTPs

NTP

TFTP –(Rivial File Transfer Protocol)

SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

The Simple Network Management Protocol (SNMP) is a framework for managing devices in an internet using the TCPIIP protocol suite. It provides a set of fundamental operations for monitoring and maintaining an internet.



Here, are some important differences between the OSI & TCP/IP model:

OSI Model	TCP/IP model
OSI model provides a clear distinction between interfaces, services, and protocols.	TCP/IP doesn't offer any clear distinguishing points between services, interfaces, and protocols.
OSI uses the network layer to define routing standards and protocols.	TCP/IP uses only the Internet layer.
OSI model use two separate layers physical and data link to define the functionality of the bottom layers	TCP/IP uses only one layer (link).
OSI model, the transport layer is only connection-oriented.	A layer of the TCP/IP model is both connection-oriented and connectionless.
In OSI model, data link layer and physical are separate layers.	In TCP data link layer and physical layer are combined as a single host-to-network layer.
The minimum size of the OSI header is 5 bytes.	Minimum header size is 20 bytes.

Client-Server Architecture

The Client-server model is a distributed application structure that partitions task or workload between the providers of a resource or service, called servers, and service requesters called clients. In the client-server architecture, when the client computer sends a request for data to the server through the internet, the server accepts the requested process and deliver the data packets requested back to the client. Clients do not share any of their resources. Examples of Client-Server Model are Email, World Wide Web, etc.

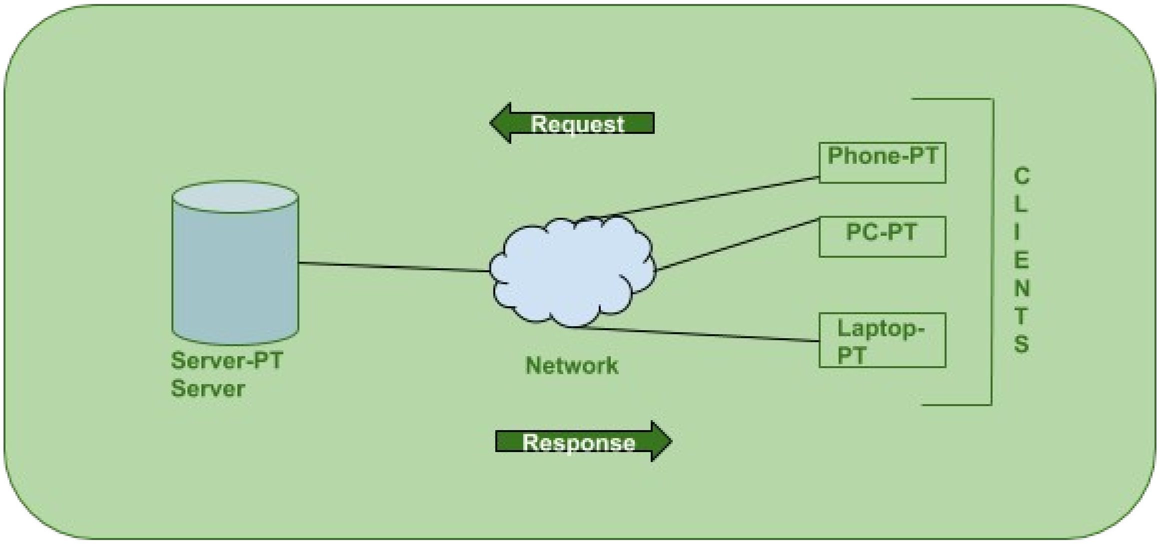
How the Client-Server Model works ?

In this article we are going to take a dive into the **Client-Server** model and have a look at how the **Internet** works via, web browsers. This article will help us in having a solid foundation of the WEB and help in working with WEB technologies with ease.

- **Client:** When we talk the word **Client**, it mean to talk of a person or an organization using a particular service. Similarly in the digital world a **Client** is a computer (**Host**) i.e. capable of receiving information or using a particular service from the service providers (**Servers**).

- **Servers:** Similarly, when we talk the word **Servers**, It mean a person or medium that serves something. Similarly in this digital world a **Server** is a remote computer which provides information (data) or access to particular services.

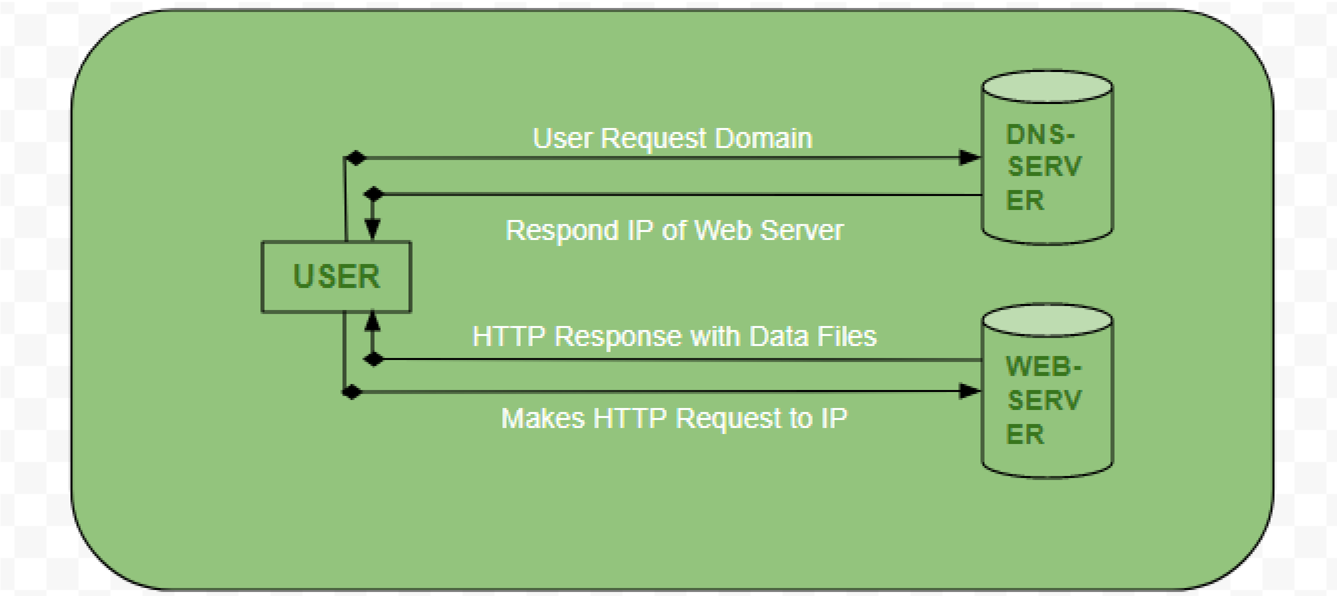
So, its basically the **Client** requesting something and the **Server** serving it as long as its present in the database.



How the browser interacts with the servers ?

There are few steps to follow to interacts with the servers a client.

- User enters the **URL**(Uniform Resource Locator) of the website or file. The Browser then requests the **DNS**(DOMAIN NAME SYSTEM) Server.
- **DNS Server** lookup for the address of the **WEB Server**.
- **DNS Server** responds with the **IP address** of the **WEB Server**.
- Browser sends over an **HTTP/HTTPS** request to **WEB Server's IP** (provided by **DNS server**).
- Server sends over the necessary files of the website.
- Browser then renders the files and the website is displayed. This rendering is done with the help of **DOM** (Document Object Model) interpreter, **CSS** interpreter and **JS Engine** collectively known as the **JIT** or (Just in Time) Compilers.



Advantages of Client-Server model:

- Centralized system with all data in a single place.
- Cost efficient requires less maintenance cost and Data recovery is possible.
- The capacity of the Client and Servers can be changed separately.

Disadvantages of Client-Server model:

- Clients are prone to viruses, Trojans and worms if present in the Server or uploaded into the Server.
- Servers are prone to Denial of Service (DOS) attacks.
- Data packets may be spoofed or modified during transmission.
- Phishing or capturing login credentials or other useful information of the user are common and MITM(Man in the Middle) attacks are common.

Sockets

IPC (Inter Process Communication) with sockets is very common in distributed systems. In nutshell, a socket is a pair of an IP address and a port number. For two processes to communicate, each of them needs a socket.

When server daemon is running on a host, it is listening to its port and handles all requests sent by clients to the port on the host (server socket).

A client must know IP and port of the server (server socket) to send a request to it. Client's port is often provided by OS kernel when client starts communication with the server and is freed when communication is over.

Although communication using sockets is common and efficient, it is considered low level, because sockets only allow transfer of unstructured stream of bytes between processes. It is up to client and server applications to impose a structure on the data passed as byte stream.

Remote Procedure Calls

RPC is a higher level communication method. It was designed to mimic procedure call mechanism, but execute it over network. RPC is conceptually similar to message passing IPC and is usually built on top of socket communication.

In contrast to IPC messages, RPC messages are well structured. Each message includes information about function to be executed and the parameters to be passed to that function. When the function is executed, a response with output is sent back to the requester in a separate message.

RPC hides the details of communication by providing a stub on the client side. When client needs to invoke a remote procedure, it invokes the stub and pass it the parameters. The stub marshals the parameters and sends a message to RPC daemon running on the server. RPC daemon (a similar stub on the server side) receives the message and invokes the procedure on the server. Return values are passed back to the client using the same technique.

Pipes

Pipe is one of the oldest and simplest IPC methods, that appeared in early UNIX systems. A pipe is an IPC abstraction with two endpoints, similar to a physical pipe. Usually one process puts data to one end of the pipe and another process consumes them from the other one.

Ordinary pipes

Ordinary pipes are unidirectional, i.e. allow only one-way communication. They implement standard producer-consumer mechanism, where one process writes to the pipe and another one reads from it. For two-way communication two pipes are needed.

Ordinary pipes require a parent–child relationship between communicating processes, because a pipe can only be accessed from process that created or inherited it. Parent process creates a pipe and uses it to communicate with a child created via *fork()*. Once communication is over and processes terminated, the ordinary pipe ceases to exist.

Named pipes

Named pipes are more powerful. They do not require parent–child relationship and can be bidirectional. Once a named pipe is created, multiple non related processes can communicate over it.

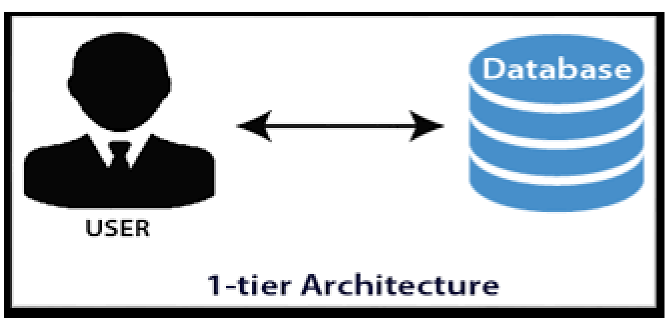
Named pipe continues to exist after communicating processes have terminated. It must be explicitly deleted when not required anymore.

Architectural patterns for distributed systems

Common **architectural patterns** for organizing the architecture of a distributed system:

1-Master-slave architecture (1-tier Model)

Master-slave architectures are commonly used in real-time systems in which guaranteed interaction response times are required. There may be separate processors associated with data acquisition from the system's environment, data processing and computation and actuator management. The ***'master' process is usually responsible for computation***, coordination and communications and it controls the 'slave' processes. ***'Slave' processes are dedicated to specific actions***, such as the acquisition of data from an array of sensors.



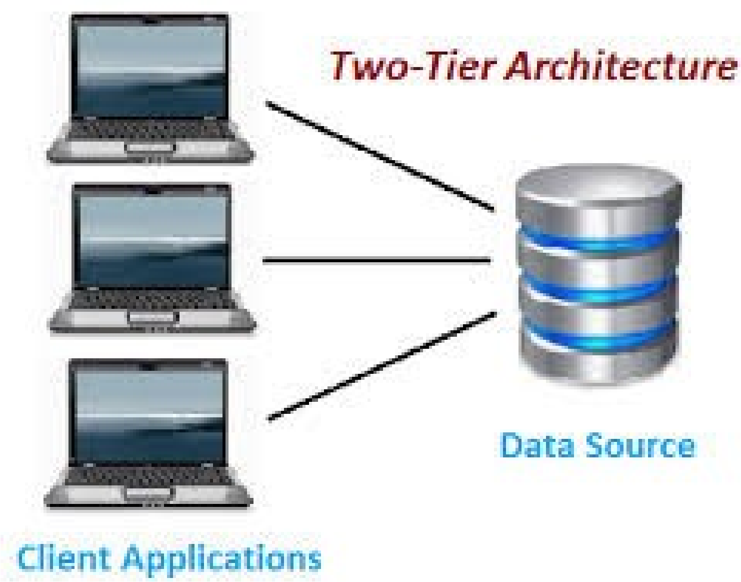
2-Two-tier client-server architecture

In a two-tier client-server architecture, the system is implemented as a single logical server plus an indefinite number of clients that use that server.

Thin-client model where the presentation layer is implemented on the client and all other layers (data management, application processing and database) are implemented on a server. There are very few thin-client applications with all processing carried out on remote server.

Fat-client model, where some or all of the application processing is carried out on the client. Data management and database functions are implemented on the server.

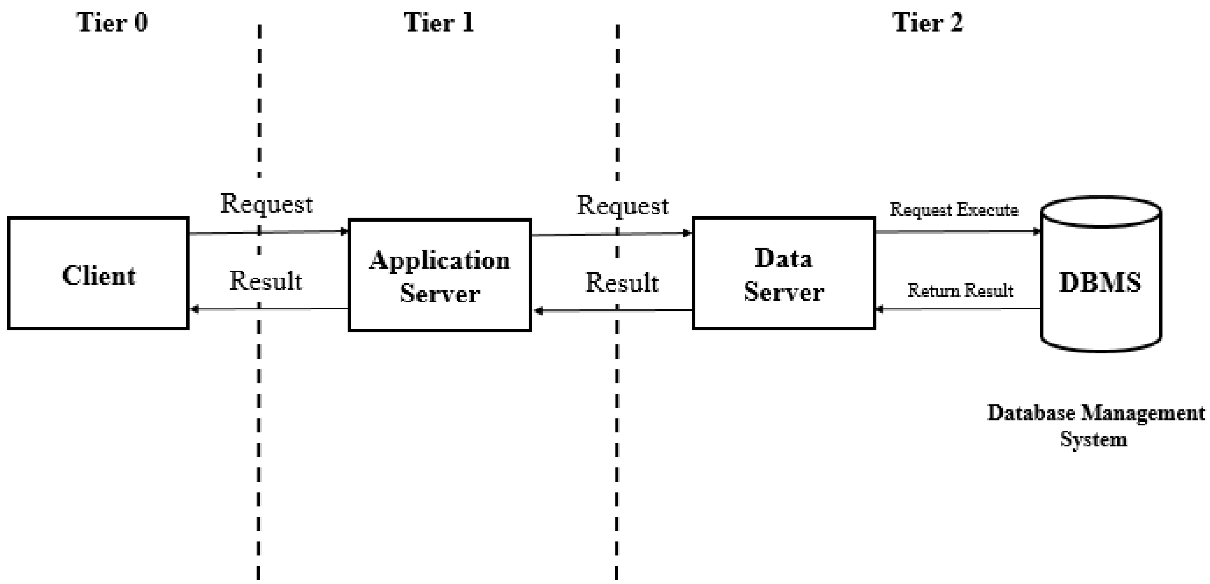
However, the distinction between thin and fat client architectures has become blurred. Java script allows local processing in a browser so some parts of a 'fat-client' functionality can be made available without software installation. Mobile apps carry out some local processing to minimize demands on network. Auto-update of apps reduces management problems.



3-Multi-tier client-server architecture

In a multi-tier client-server architecture, the different layers of the system, namely presentation, data management, application processing, and database, are separate processes that may execute on different processors. This avoids problems with scalability and performance if a thin-client two-tier model is chosen, or problems of system management if a fat-client model is used.

Use case: when there is a high volume of transactions to be processed by the server.



4-tier-Distributed component architecture (N-tier)

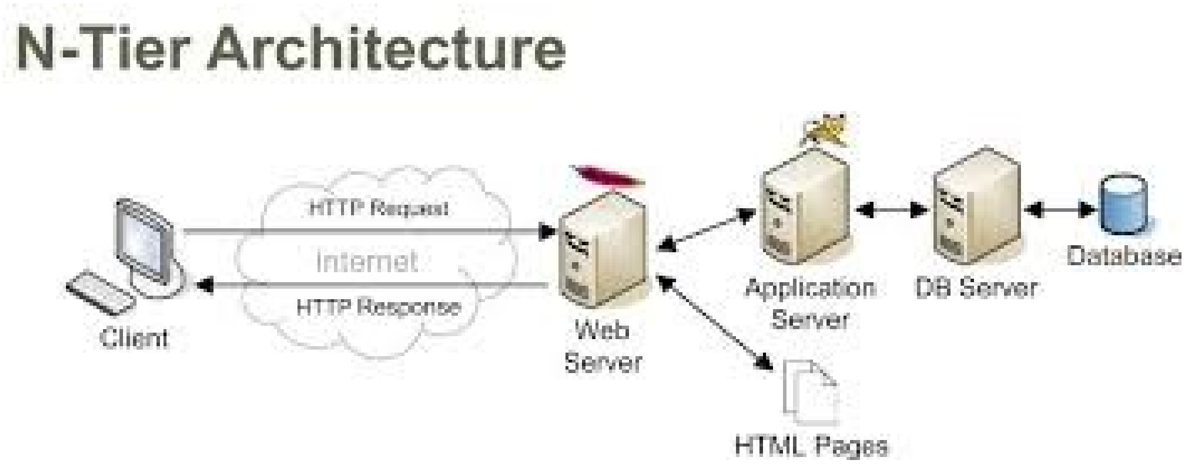
There is no distinction in a distributed component architecture between clients and servers. Each distributable entity is a component that provides services to other components and receives services from other components. Component communication is through a middleware system. Used when resources from different systems and databases need to be combined, or as an implementation model for multi-tier client-server systems. Benefits include:

- It allows the system designer to delay decisions on where and how services should be provided.
- It is a very open system architecture that allows new resources to be added as required.
- The system is flexible and scalable.
- It is possible to reconfigure the system dynamically with objects migrating across the network as required.

Distributed component architectures suffer from two major disadvantages:

- They are more complex to design than client-server systems. Distributed component architectures are difficult for people to visualize and understand.
- Standardized middleware for distributed component systems has never been accepted by the community. Different vendors, such as Microsoft and Sun, have developed different, incompatible middleware.

As a result of these problems, service-oriented architectures are replacing distributed component architectures in many situations.



5-Peer-to-peer architecture

Peer to peer (p2p) systems are decentralised systems where computations may be carried out by any node in the network. The overall system is designed to take advantage of the computational power and storage of a large number of networked computers.

Most p2p systems have been personal systems but there is increasing business use of this technology. Used when clients exchange locally stored information and the role of the server is to introduce clients to each other. Examples:

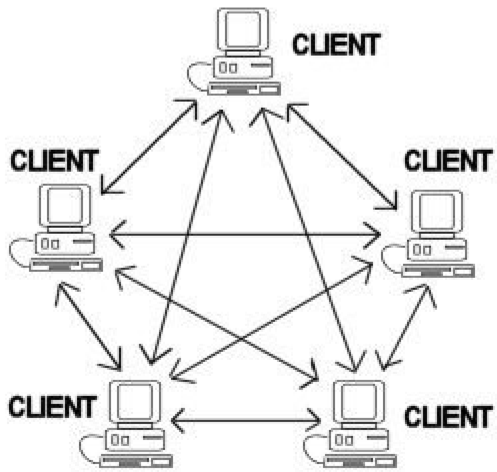
- File sharing systems based on the Bit Torrent protocol
- Messaging systems such as Jabber
- ***Payments systems, e.g. Bitcoin***
- Databases, e.g. Freenet is a decentralized database
- Phone systems, e.g. Viber
- Computation systems

P2P architectures are used when

- A system is computationally-intensive and it is possible to separate the processing required into a large number of independent computations.
- A system primarily involves the exchange of information between individual computers on a network and there is no need for this information to be centrally-stored or managed.

Security issues:

- Security concerns are the principal reason why p2p architectures are not widely used.
- The lack of central management means that malicious nodes can be set up to deliver spam and malware to other nodes in the network.
- P2P communications require careful setup to protect local information and if not done correctly, then this is exposed to other peers.



Components of client server architecture:

Essentially, three components are required to make client server architecture work. The three components are workstations, servers, and networking devices. Let us, now, discuss them in detail:

- Workstations: Workstations are also called client computers. Workstations work as subordinates to servers and send them requests to access shared files and databases. A server requests information from the workstation and performs several functions as a central repository of files, programs, databases, and management policies. Workstations are governed by server-defined policies.
- Servers: Servers are defined as fast processing devices that act as centralized repositories of network files, programs, databases, and policies. Servers have huge storage space and robust memory to deal with multiple requests, approaching simultaneously from various workstations. Servers can perform many roles, such as mail server, database server, file server, and domain controller, in client server architecture at the same time.
- Networking devices: Now that we know about the roles that workstations and servers play, let us learn about what connects them, networking devices. Networking devices are a medium that connects workstations and servers in client server architecture. Many networking devices are used to perform various operations across the

network. For example, a hub is used for connecting a server to various workstations. Repeaters are used to effectively transfer data between two devices. Bridges are used to isolate network segmentation.